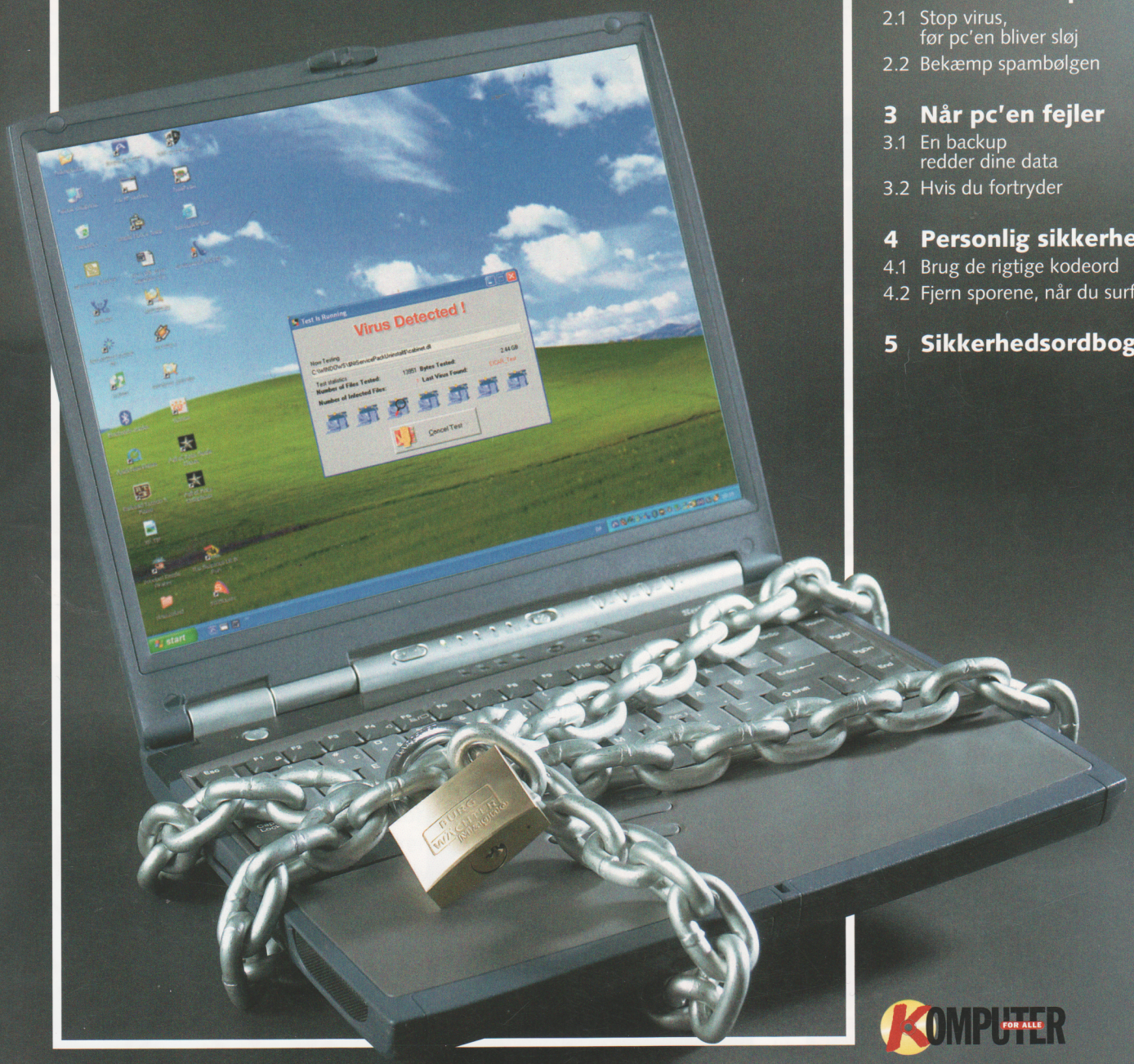
SIKKER PC

Alle programmerne i dette sikkerhedstema er gratis og ligger på Sikkerheds-cd'en, som følger med dette hæfte!



1 Når du surfer 4
1.1 Hold hackerne ude
1.2 Fjern reklamer og skumle spioner
1.3 Gode gratis råd

2 Trusler med posten 12
2.1 Stop virus, før pc'en bliver sløj
2.2 Bekæmp spambølgen

3 Når pc'en fejler 18
3.1 En backup redder dine data
3.2 Hvis du fortryder

4 Personlig sikkerhed 22
4.1 Brug de rigtige kodeord
4.2 Fjern sporene, når du surfer

5 Sikkerhedsordbog 26

KOMPUTER FOR ALLE

BESTIL KOMPUTER IDAG
PÅ TLF. 39 10 30 72
www.komputer.dk

Bring computeren i sikkerhed for trusler både inde- og udefra

Ved hjælp af en række hjælpeprogrammer og en god portion sund fornuft kan du forsvare dig mod alt fra virusangreb til systemnedbrud. Vi viser dig her, hvordan du gør.

Verden er ikke ond. Grundlæggende er Jorden et venligt sted, og de fleste folk vil gerne hjælpe hinanden. Desværre er der også derude en del tvivlsomme eksistenser, der ikke har opdaget den ovenstående sandhed – og dem skal man passe virkelig godt på ikke at give en chance for at lave numre!

Det lyder måske som den rene paranoia, men det handler i virkeligheden blot om sund fornuft og grundig forberedelse. De fleste farer – både de menneskeskabte og de mere tilfældige – kan nemlig forebygges og forhindres.

På *Komputer for alle* har vi samlet de bedste gratis sikkerhedsprogrammer til din pc. Med dem installeret på computeren og med dette hæfte i hånden er du klædt virkelig godt på til at modstå alle de stød og ubehageligheder, som verden giver din kære elektroniske ven.

PAS GODT PÅ!

De værste trusler mod computeren

VIRUS: En 20 år gammel trussel Hvis du tror, at ubehageligheder som computervirus er en moderne foreteelse, må du tro om. Computervirus som begreb har lige haft 20-års jubilæum. Så længe siden er det, at en amerikansk studerende ved navn Fred Cohen lavede den første af slagsen i et lukket laboratorieeksperiment som en del af sin ph.d.-afhandling. Den første "vilde" virus blev fundet tre år senere, i 1986. I dag findes der ca. 60.000 virus i omløb, så et godt antivirusprogram er en simpel nødvendighed.

SPAM: 25 år med uønskede reklamer En anden af internettets plageånder har også haft jubilæum for nylig. Spam – i betydningen uønsket reklamepost, udsendt til mange modtagere – blev første gang oplevet d. 1. maj 1978, hvor computerproducenten DEC sendte en invitation om et åbent hus-arrangement ud til omkring 1000 intetanende modtagere. Første gang ordet "spam" blev brugt, var dog d. 31. marts 1993, hvor udtrykket blev brugt af Joel Furr. Det blev straks taget op, og den uheldige ophavsmand til reklamebudskabet undskyldte samme dag på nettet, at han havde udsendt spam. På det tidspunkt havde han modtaget over 200 klagebreve.

HACKERE: Fra hobbyfolk til kriminelle Ordet "hacker", som vi i dag forbinder med skumle typer, der prøver at bryde ind på computeren, havde oprindelig en ganske anden og mere fredelig betydning, nemlig en person, som går virkelig meget op i programmering og computere. Og udtrykket at hacke dækkede dengang – i 1960'erne – over det at programmere eller på anden måde beskæftige sig intenst med computere. Disse folk benævner stadig sig selv som hackere, mens de bruger ordet "crackere" om de folk, som bryder loven.

HARDDISKEN: Pc'ens svageste led Mens CPU og grafikkort næsten altid kan holde i årevis, efter at de er blevet kasseret på grund af forældelse, må du regne med at opleve, at en harddisk opgiver ævred fra tid til anden. En harddisks forventede levetid opgives fra producenten med tallet MTBF (Mean Time Between Failures eller gennemsnitlig tid mellem fejl), og tallet er gerne mindst 500.000 timer. Så man skulle tro, at disken kunne fortsætte i årtier. Men praksis og teori er to forskellige størrelser, og folk, der lever af at vedligeholde pc-udstyr, siger, at du skal være heldig, hvis du har harddisken i op til fem år!

... og det mest populære forsvar

FIREWALLS: Fra big business til hyldevare. En firewall var tidligere synonymt med en særlig computer, der stod som en vogter mellem virksomhedens netværk og internettet. Og det var kun virksomheder med betydningsfulde data, som havde grund til at have en firewall. I dag har selv ganske almindelige private computerejere brug for beskyttelse mod angreb fra internettet. Til gengæld kan opgaven klares af et program, som tilmed kan fås ganske gratis.

SIKKER PC
Udgivet af Komputer for alle som tillæg til Komputer for alle 4/2004

Forfatter: John Alex Hvidlykke
Fotos: Hem Fotografi
Layout: Thomas Brandstrup
Ansvarshavende udgiver: Jens Henneberg
Tryk: Johler Druck GmbH, Neumünster

Komputer for alle udgives af
Bonnier Publications International AS
Kirkegaten 20, N-0153 Oslo
© 2004 Bonnier Publications International AS

1

NÅR DU SURFER

Når din pc er på internettet, er den udsat for en verden af farer. Programmer, som virker uskyldige, kan indeholde mere, end de giver udtryk af. Hackere kan trænge ind i din pc og gennemrode harddisken – eller kidnappe pc'en og bruge den som en digital rambuk mod andre computere. I mindre dramatiske tilfælde bliver du overhældt med reklamer, takket være små ekstra "serviceprogrammer", som installeres uden din viden og accept.

I dette kapitel bygger vi et værn om pc'en mod internettets uønskede elementer og sætter et "nej tak til reklamer"-skilt på døren. Og når pc'en er beskyttet, smider vi uønskede spioner og snushaner ud ad vinduet. Du får også gode råd og hjælpemidler til at holde øje med, at alting er, som det burde være.

Her er truslerne

Noget af det mest spændende – og farligste – du kan gøre med en pc, er at gå på internettet. Det åbne cyberspace er desværre opholdssted for nogle af planetens største plattenslagere. Hackere betragter din tilstedeværelse på internettet som en åben invitation til at ransage din pc, og verdens mest skrupelløse reklamefolk fylder din computer med spionprogrammer, så de kan lære mest muligt om dig og dine vaner. Endelig er der dem, som så gerne vil have din opmærksomhed og dine penge, at de er parate til at kidnappe enten din browser eller dit modem.

Byg en brandmur om din computer

En firewall styrer al trafik til og fra internettet og holder samtidig hackere effektivt ude.

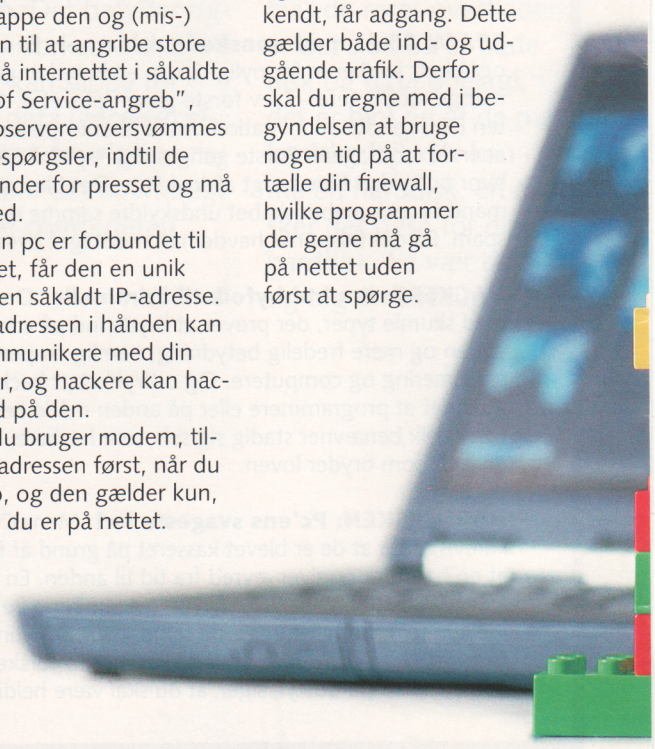
For få år siden var en firewall noget, som kun interesserede større virksomheder med store computere. Kun her var der noget at hente for hackere, som brugte dage på at trænge ind via telefonnettet. Det var dengang. I dag er selv private computere udsat for hackerangreb. Det verdensomspændende internet har gjort det let for hackere at bevæge sig fra computer til computer, og hurtige, permanente netforbindelser med ADSL eller kabelmodem har gjort private pc'er interessante at trænge ind på.

De færreste af os ligger inde med statshemmeligheder på hjemme-pc'en, men hackere kan kidnappe den og (mis-) bruge den til at angribe store servere på internettet i såkaldte "Denial of Service-angreb", hvor webservere oversvømmes med forespørgsler, indtil de bukker under for presset og må lukkes ned.

Når din pc er forbundet til internettet, får den en unik adresse, en såkaldt IP-adresse. Med IP-adressen i hånden kan man kommunikere med din computer, og hackere kan hacke sig ind på den.

Hvis du bruger modem, tildeles IP-adressen først, når du ringer op, og den gælder kun, så længe du er på nettet. Næste gang får du sandsynligvis en ny. Derfor er det så godt som umuligt for hackere at finde frem til din pc. Med ADSL og kabelmodem er det en ganske anden sag. Her er adressen i nogle tilfælde fast (afhænger af din udbyder), eller pc'en har i hvert fald samme adresse, så længe du er på nettet, hvilket vil sige, lige så længe pc'en er tændt.

Løsningen på hackertruslen er en firewall. En firewall er et stykke hardware eller et program, som fungerer som "dørmand" mellem internettet og din pc. Al kontakt til og fra nettet skal gennem firewallen, og kun de, der bliver godkendt, får adgang. Dette gælder både ind- og udgående trafik. Derfor skal du regne med i begyndelsen at bruge nogen tid på at fortælle din firewall, hvilke programmer der gerne må gå på nettet uden først at spørge.



Om Agnitum Outpost Firewall Free Edition

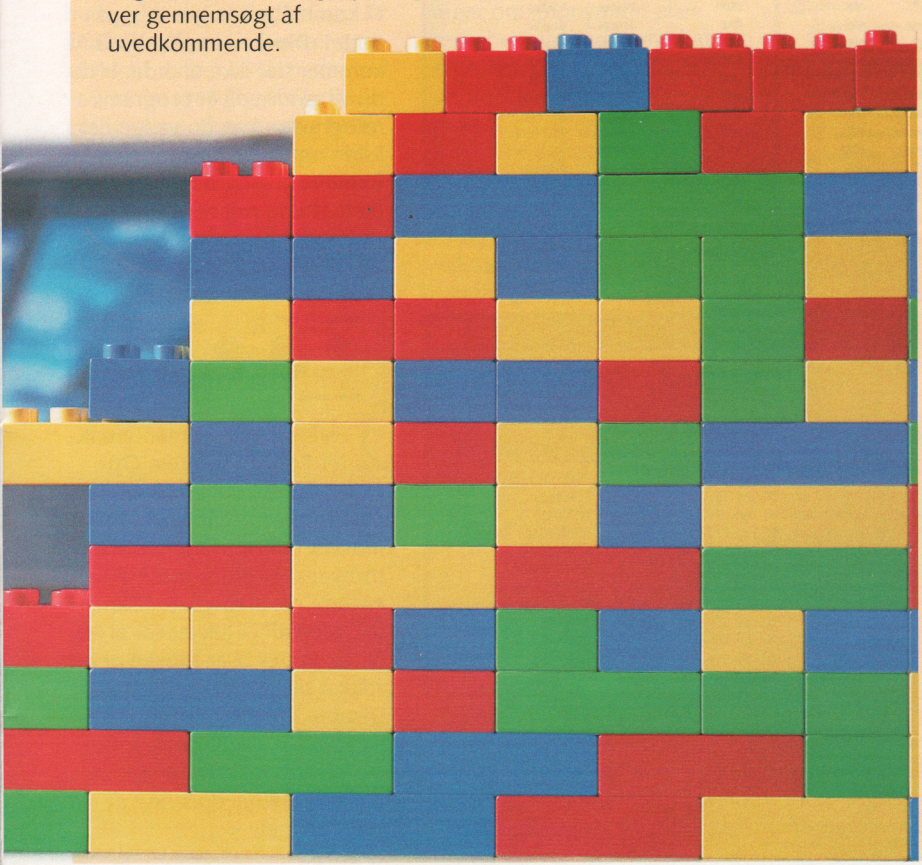
På *Komputer for alles* Sikkerheds-cd finder du programmet *Agnitum Outpost Firewall Free Edition*, som er en meget omfattende og ganske gratis firewall. Oven i normale firewall-funktioner (som at holde hackere ude) indeholder *Outpost* også en række filtre mod andre af nettets ubehagligheder: Pop-up-reklamer, bannerreklamer og visse typer af spam. Det bedste af det hele er, at programmet er relativt let at gå til. De vigtigste funktioner fungerer, fra det øjeblik programmet er installeret. Du skal dog stadig bruge lidt tid på at "træne" *Outpost* til at kende dine internet-programmer.

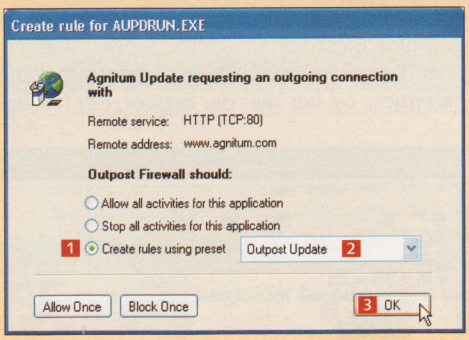
■ Ud over selve firewall-programmet *Outpost* finder du også en komplet, engelsksproget manual til programmet på cd'en. Manualen er i pdf-format og kan læses på skærmen med Acrobat Reader eller printes ud (100 sider!).

Hr. lærer – må jeg gå på nettet?

Når *Outpost* starter op, sker det med regelsættet "Rules Wizard". Det betyder, at den prøver at lære at lave regler for adgangen til internettet. Derfor vil du i begyndelsen blive mødt med spørgsmål, hver gang et nyt program vil bruge internettet (fx når du vil modtage eller sende e-mail). Du kan vælge, at programmet altid skal have fuld internetadgang, blokeres helt altid, eller du kan definere, under hvilke omstændigheder programmet skal have lov til at sende og modtage data over nettet. Til det formål findes en række skabeloner med typiske "rettigheder" for programmer. Du kan også vælge blot at give adgang eller spærre denne ene gang. Men det betaler sig ikke, da de fleste programmer vil reagere på en afvisning med at prøve igen – og så får du spørgsmålet igen!

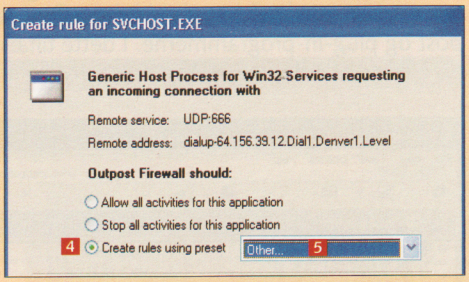
Det siger sig selv, at både dit mailprogram og din browser skal have lov til at gå på nettet, hvis du skal have gavn af dem, men hvad med for eksempel Word? Og hvad med det gratis program, som du hentede og installerede i går. Skal de også have lov til at "ringe hjem"? Hvis du er i tvivl, er det bedre at sige nej en gang for meget end en gang for lidt. For en firewall, som tillader al trafik, er ikke en firewall, men en svingdør. Hvis du kommer til at blokere for et program, som har brug for nettet, kan du altid ændre på indstillingerne, når programmet nægter at fungere. Til gengæld er det ikke sikkert, at du opdager det, hvis du siger ja en gang for meget, og din harddisk lige så stille bliver gennemsøgt af uvedkommende.



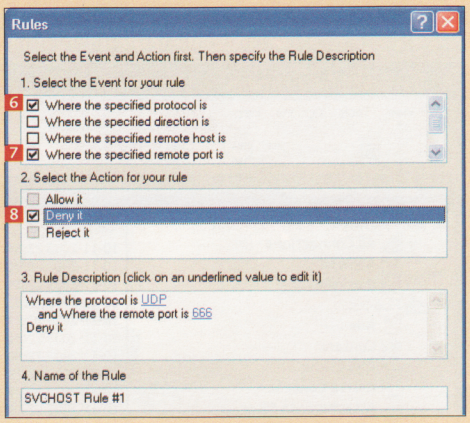


1 Her er et "ukendt" program på vej på nettet. Heldigvis er det blot *Outpost*, som leder efter en opdatering. Det må den godt. Vælg **Create rules using preset** 1, vælg reglen **Outpost Update** 2 fra listen, og klik på **OK** 3.

Et af de mest snakkesalige programmer er SVCHOST, som er en tjeneste under *Windows XP*. Programmet bruges til mange slags netkommunikation. Det ved hackerne desværre også. Derfor skal du ikke uden videre give programmet lov til hvad som helst.



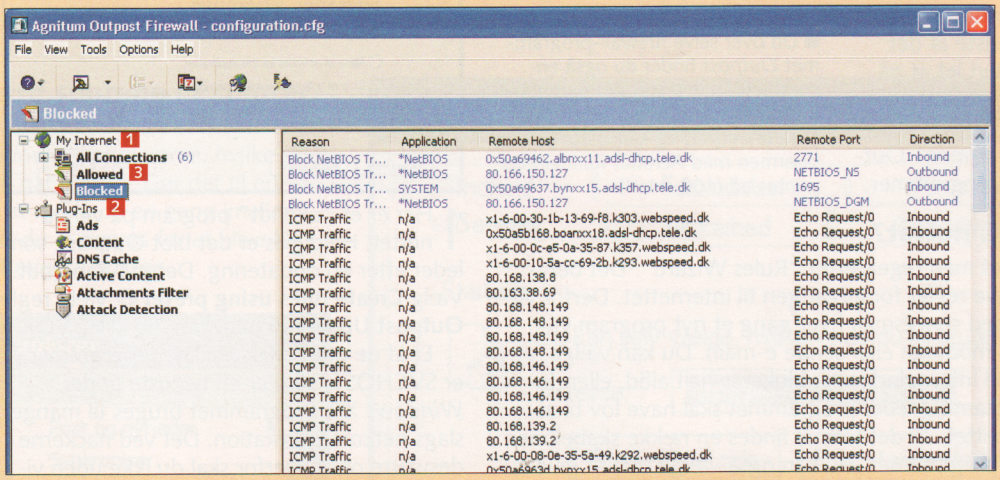
2 Her er en forespørgsel fra programmet SVCHOST, som ønsker forbindelse til internettet – og et opkald til port 666 fra et modem i Denver er et tilbud, vi ikke kan sige ja til. Desværre går det heller ikke at lukke helt for programmet, da det også bruges til legale formål. Vælg **Create rules using preset** 4, **Other** 5, og klik på **OK**.



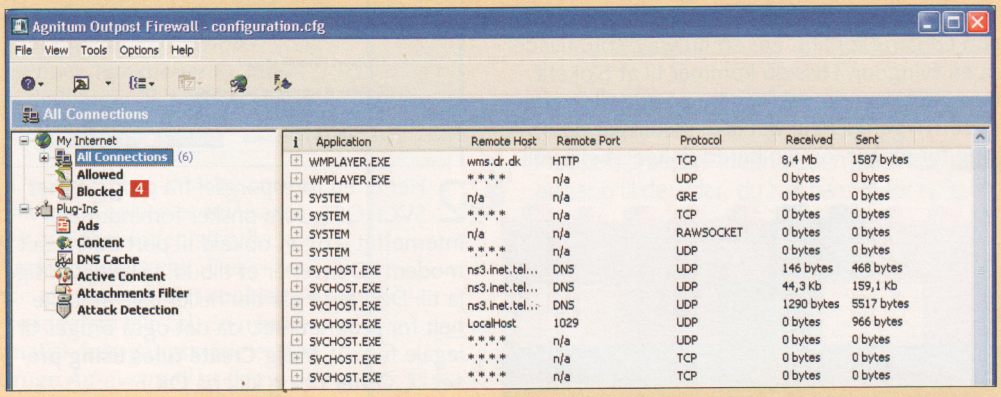
3 Nu kan du vælge mellem forskellige egenskaber. Vi har valgt **Where the specified protocol is** 6, **Where the specified remote port is** 7, og **Deny it** 8. Nu vil programmet fortsat fungere, indtil nogen spørger om adgang via port 666, som er lukket.

Sådan fungerer Agnitum Outpost

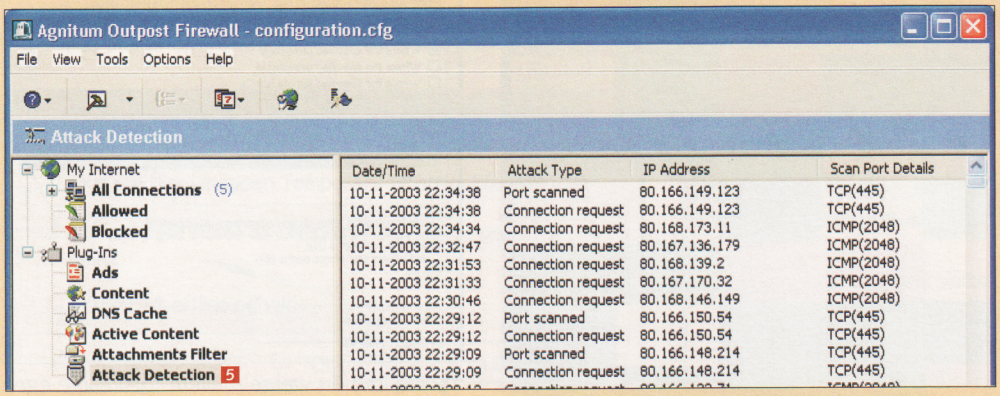
Når dine mest nethungrende programmer er registreret, mærker du ikke meget til *Outpost*. Men hvis du dobbeltklikker på spørgsmålstegnikonet i **Systembakken**, får du programvinduet på skærmen, og her sker der masser, der har betydning for, hvor sikker din pc er.



1 I vinduet til venstre kan du se to lister. Den ene, **My Internet** 1 viser alle netforbindelser, siden pc'en blev tændt. Den anden, **Plug-Ins** 2, viser en oversigt over plug-in-programmerne til *Outpost*. I det højre vindue kan du se de forbindelser og filer, der er blevet behandlet af *Outpost* og plug-in-programmerne. I dette tilfælde ses en komplet liste over forbindelsesforsøg. Hvis du klikker på **Allowed** 3, kan du se, hvilke af disse, som fik lov til at passere gennem firewallen.



2 Vælger du **Blocked** 4, kan du se alle de forsøg, som blev afvist – og hvorfor. Det er her, man får den første forsmag på, hvor meget støj og snavs, der egentlig er på internettet.

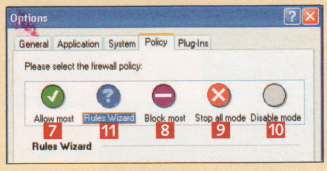


3 Hvis man klikker på **Attack Detection** 5, er der risiko for at miste tiltroen til sine medmennesker. Her får man nemlig en liste over alle angrebsforsøg at se. Et angrebsforsøg vil her sige et forsøg på at skabe forbindelse til pc'en eller en forespørgsel til, om denne eller hin port findes og er åben (en såkaldt portskanning). Den slags "indbrudforsøg" sker hele tiden. Heldigvis er det ikke alle sammen hackere. En del af dem vil bare spionere på dig og sende dig spam!

De vigtigste indstillinger i Outpost

Antallet af indstillingsmuligheder er nærmeste astronomisk, og der er god grund til, at manualen fylder 100 sider. Heldigvis kan programmet bruges, uden at du behøver kende samtlige funktioner til bunds. Du får lettest adgang til indstillingerne med menuen **Options**.

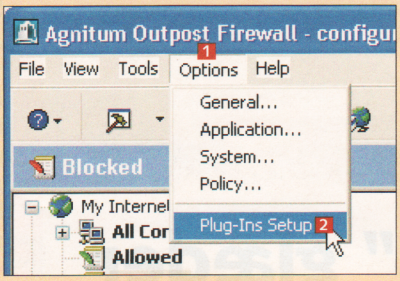
1 Hvis du vælger **Options**, **Application** 1, får du en oversigt over, hvilke programmer programmet har til- og mistro til. **Trusted applications** 2 får lov til alt på nettet, mens **Partially allowed applications** 3 kun må gøre visse ting på nettet. **Blocked applications** 4 kommer slet ikke til orde. Hvis du vil ændre på et programs rettigheder, kan du vælge det i listen og vælge **Edit** 5. Eller **Remove** 6 – og begynde forfra med at lave regler.

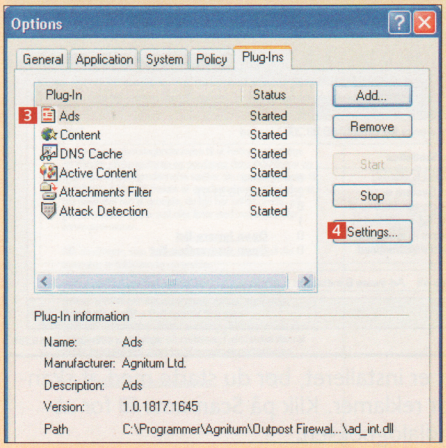


2 Hvis du vælger menupunktet **Policy** i menuen **Options**, kan du vælge firewallens beskyttelsesniveau – fra **Allow most** 7 (alt er tilladt, indtil det forbydes) til **Block most** 8 (alt er forbudt, til du giver tilladelse). **Stop all** 9 lukker for al trafik og svarer til at trække netstikket ud af væggen, mens **Disable** 10 åbner for alle sluser. Det bedste kompromis er **Rules Wizard** 11, selv om det indebærer en del oplæring af programmet.

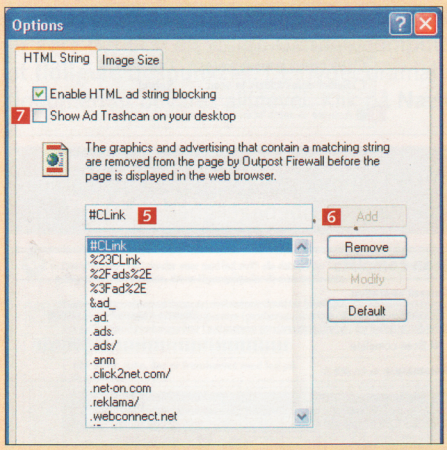
Plug-ins i Outpost

Agnitum Outpost har en funktion, som adskiller den fra andre firewalls: Man kan udvide programmet med plugin-programmer. På samme måde, som du måske kender det fra fx *Internet Explorer* eller *Winamp*. På den måde kan andre firmaer udvikle udvidelser, som føjer nye funktioner til programmet. Der følger seks plug-ins med *Outpost*: **Ads, Content, DNS Cache, Active Content, Attachments Filter** og **Attack Detection**. Du kan indstille programmerne ved at vælge menuen **Options** 1, **Plug-Ins Setup** 2.



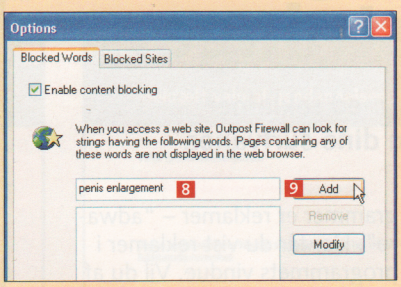


1 Nu får du dialogboksen **Options** på skærmen, med fanen **Plug-Ins** valgt. Du kan indstille hver plug-in ved at vælge den i vinduet til venstre 3 og klikke på knappen **Settings** 4. Her gennemgås de vigtigste indstillinger:

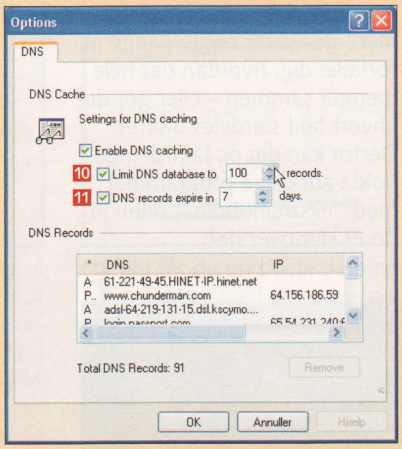


2 Plug-in-programmet *Ads* kan filtrere uønskede annoncer fra websider, så du både slipper for synet af dem og sparer den tid, som det tager at hente dem. Annoncer kan både genkendes på billedernes størrelse og de adresser og nøgleord, som optræder i HTML-koden på hjemmesiderne. Hvis du møder en webadresse, som udsender særlig mange annoncer, kan du skrive adressen i tekstfeltet 5 og klikke på **Add** 6. Du kan også anbringe et lille skraldespandsikon på skærmen (**Show Ad Trashcan**) 7, som du simpelt hen kan trække annoncebillederne over i.

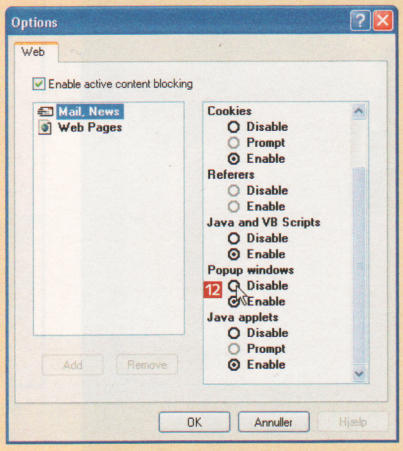
3 Plug-in-programmet *Content* kan spærre for hjemmesider med indhold, som du ikke ønsker at se på. Skriv dine yndlingshadeord i tekstfeltet 8, og klik på **Add** 9.

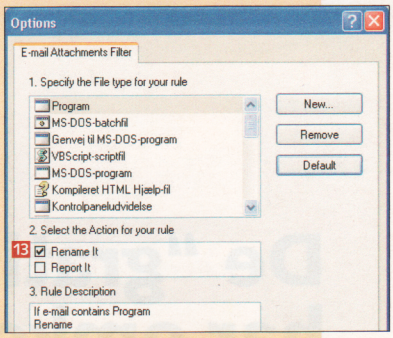


4 Plug-in'en *DNS Cache* handler ikke om at fjerne noget, men tværtimod om at gøre det lettere. Programmet husker IP-adressen på de seneste besøgte websteder. På den måde slipper din pc for at bede en DNS-server om at oversætte domænenavnene til de IP-numre, som ligger bagved navnene. På fanen kan du indstille, hvor mange adresser programmet husker (**Limit DNS database to**) 10 – og hvor længe (**DNS records expire in**) 11.

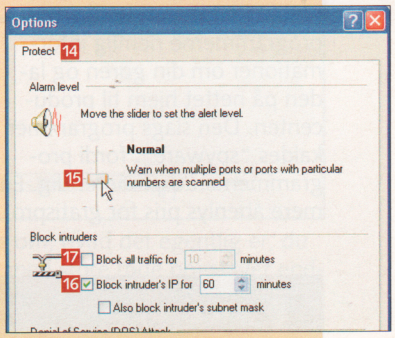


5 Hvis du er træt af pop-up-reklamer, der dukker frem på skærmen, når du besøger hjemmesider eller læser din mail, kan de fjernes med programmet *Active Content*. Her kan du slå en lang række ekstrafunktioner i mails og websider til og fra. Men husk, at den samme teknik, der giver os irriterende pop-ups 12, også nogle steder bruges til menuer.





Plug-in-programmet *E-mail Attactments Filter* kan passivisere uønskede postpakker. Fra start er alle vedhæftede filer sat til **Rename** 13. Det betyder, at svaret på alle slags vedhæftede filer vil være **Gem som**-dialogboksen, så man fx ikke i uopmærksomhed kører et ukendt program.



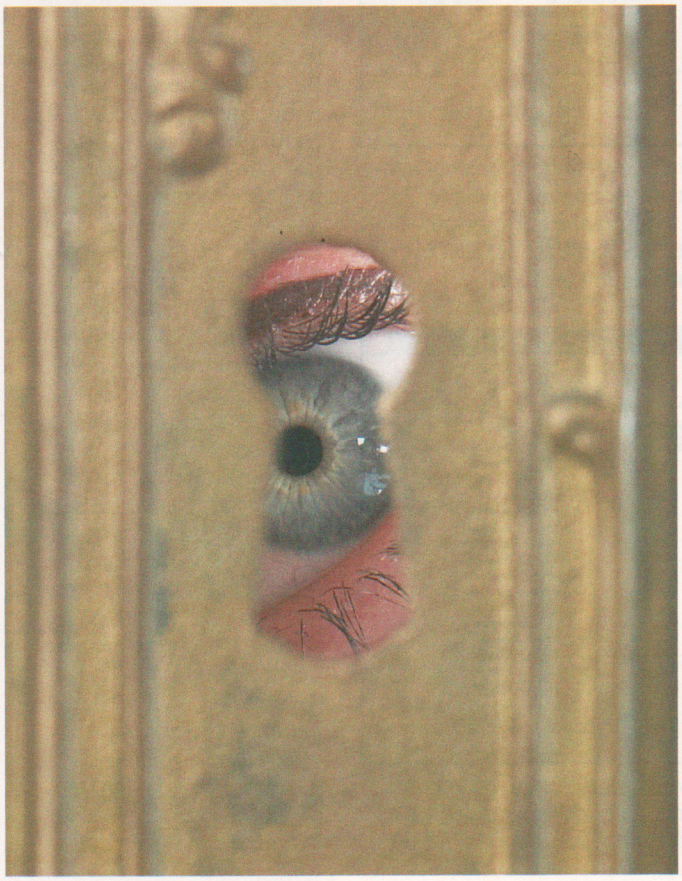
På fanen **Protect** 14 i plug-in-programmet *Attack Detection* kan du indstille, hvordan *Outpost* reagerer på angrebsforsøg. Skydeknappen **Alarm Level** 15 bestemmer, hvor nævenyttige de uindbudte gæster skal være, før du får en advarsel. **Normal** er passende, hvis du ikke vil forstyrres konstant. Den mest effektive måde at reagere på er at lukke den mistænkte ude. **Block intruder's IP for** 16 blokerer alle henvendelser fra den mistænkte adresse i en time. Så kan han skrige sig blå i hovedet, uden at vi hører det! Til gengæld vil vi fraråde at markere i feltet **Block all traffic for** 17, da den betyder, at al nettrafik, herunder browser og e-mail, afbrydes i ti minutter, når en fremmed computer, banker på. Og det rammer dig mere end hackerne!

De "gratis" glæder har omkostninger

Gratis programmer betales med reklamer – eller med oplysninger om dine surfvaner.

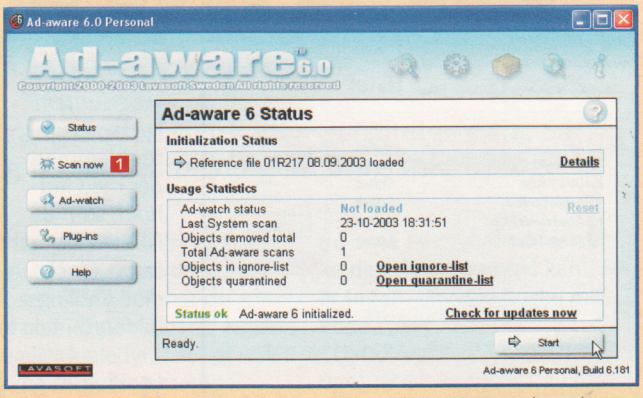
Internettet er pragtfuldt. Alting kan findes ganske gratis! Men selv programmører skal jo leve, og nogle gange har de gratis glæder derfor en skjult pris. Alt imens du surfer fornøjet på nettet, sender nogle af gratisprogrammerne nemlig informationer om din gøren og laden på nettet hjem til producenten. Den slags programmer kaldes "spyware", fordi programmerne udspionerer dig. En mere åbenlys pris for gratisprogrammer er reklamer – "adware". Her får du vist reklamer i programmets vindue. Vil du af med reklamerne, må du betale for programmet.

Programfirmaerne "glemmer" desværre nogle gange at fortælle dig, hvordan det hele hænger sammen – eller gør det i hvert fald særdeles diskret. Derfor kan din pc faktisk indeholde adskillige programmer med "ekstraindhold", uden at du er klar over det.



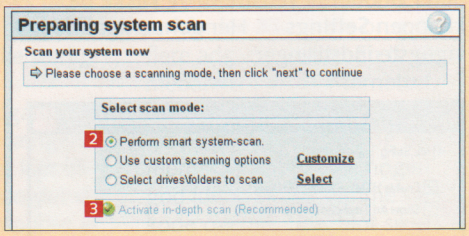
Sådan bruger du Ad-aware 6.0

Programmet *Ad-aware* ("opmærksom på reklamer") bekæmper begge typer snyltere samt en række andre. Det skanner din harddisk for og fjerner forskellige sladderhanke og ureelle programmer. Du skal dog være opmærksom på, at nogle af de gratis programmer holder op med at fungere, hvis man fjerner reklamerne, ligesom filer fra din netbank kan dukke op i oversigten. Derfor betaler det sig at gennemgå listen grundigt, inden *Ad-aware* fjerner filerne.

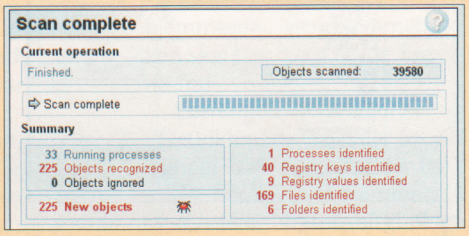


1 Når programmet er installeret, bør du starte med at skanne harddisken for reklamer. Klik på **Scan now** 1 for at komme til skanningdialogboksen.

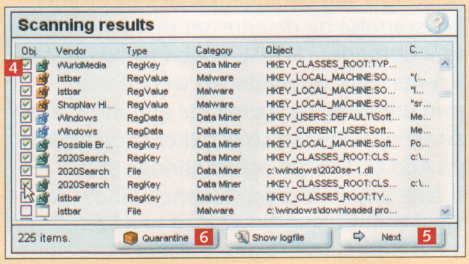
2 Standardforslaget er **Perform smart system-scan** 2. For dem, som ikke har bestået en udvidet eksamen i reklamekundskab, er det et ganske fornuftigt valg. Tjek samtidig, at der er markering ud for **Activate in-depth scan** 3. Klik på **Next**.



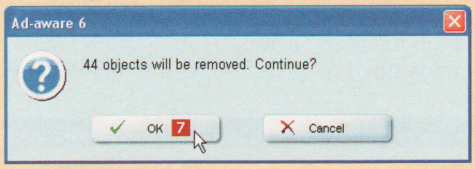
3 Efter nogle minutter kommer *Ad-aware* frem med en besked om, hvor mange slags ubehageligheder der er fundet på harddisken. Selv på en relativt jomfruelig pc kan der være ret mange. Klik på **Next** for at se listen over fundne programmer.



4 Du bliver nu præsenteret for en liste over spionprogrammer og deres anvendelse. Markér de programmer, som du ønsker at fjerne 4, og klik på **Next** 5. Hvis du er i tvivl, kan du i stedet klikke på **Quarantine** 6 og nøjes med at gemme filerne af vejen.



5 Hvis du valgte **Next** tilbage i trin 4, bliver de valgte filer nu slettet. Klik på **OK** 7. Nu er du en hel række sikkerhedsbekymringer og sladderhanke kvit.

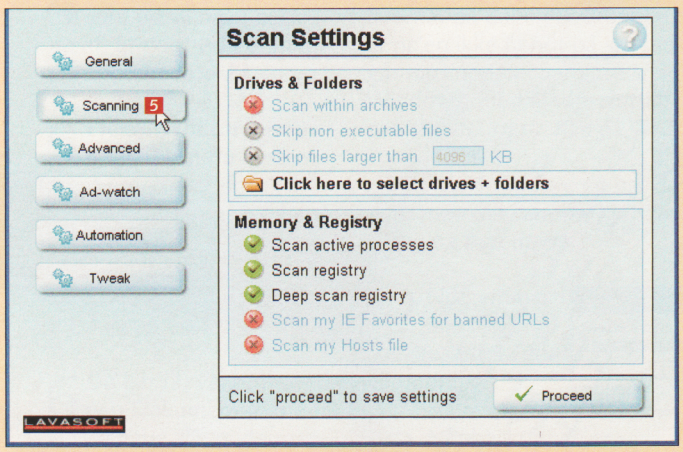


Indstillinger i Ad-aware

Hvis du har lyst til selv at rode med indstillingerne, giver *Ad-aware* rige muligheder for at pille, trimme og justere. De fleste og mest interessante findes i dialogboksen **Settings**.

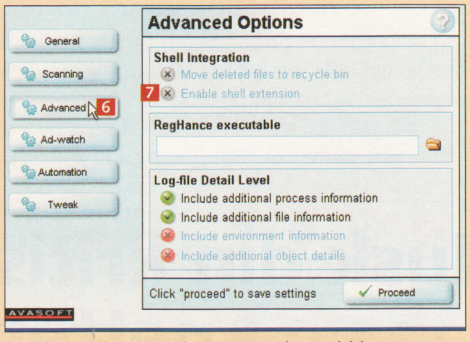
1 Klik på tandhjulsikonet for at åbne dialogboksen **Settings** 1.

2 **Settings** er opdelt i seks underpunkter. Under **General** 2 findes sprogindstillinger og placeringen af programmets logfiler. Du kan også vælge, om der skal laves en skanning, når pc'en starter, ved at klikke på **Customize** 3 – i så fald åbnes punktet **Automation** 4.



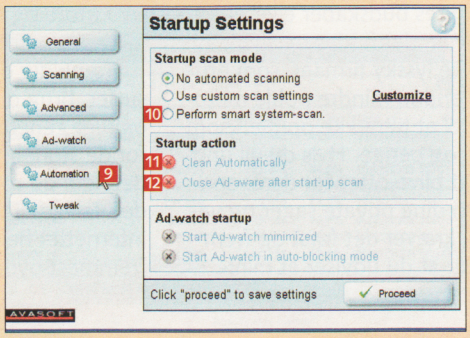
3 I punktet **Scanning** 5 kan du vælge, hvilke mapper og filer der evt. skal springes over, når systemet skannes.

4 Under **Advanced** 6 kan du vælge at få helt nøjagtige oplysninger om de forskellige fjernede spionprogrammer med i logfilen. I købeudgaven af *Ad-aware* kan man desuden vælge at indbygge skanning i højreklikmenuen i Windows (**Enable shell extension**) 7, men som almindelig bruger kan du sagtens klare dig uden denne funktion.

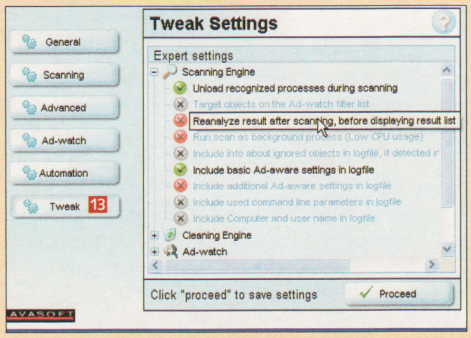


5 Indstillingsmulighederne under **Ad-watch** 8 er kun tilgængelige i købeudgaven af programmet.

6 Under **Automation** 9 kan du blandt andet indstille *Ad-aware* til automatisk at skanne systemet for spionprogrammer, hver eneste gang pc'en starter op (**Perform smart system-scan**) 10, automatisk fjerne misdæderne (**Clean Automatically**) 11 og lukke ned igen bagefter (**Close Ad-aware after start-up scan**) 12.



7 **Tweak** 13 er for de virkelig pilfingrede. Her kan du i detaljer justere den måde, *Ad-aware* skanner og renser for spionprogrammer på. Hvis du har lyst til at bruge ekstra lang tid, kan du for eksempel her vælge at lade programmet skanne systemet en ekstra gang, efter at du har fjernet spionprogrammerne.



Husk din kritiske sans på nettet

Selv om pc'en er beskyttet mod hackere og spioner, skal du stadig være på vagt, når du surfer.

Hvis du har fulgt anvisningerne indtil nu, har du nu en pc, som er godt beskyttet mod hackere og fri for luskede reklamer og spioner. Faktisk har vi elimineret de fleste udefrakommende farer. Nu mangler vi blot at se på den største risiko for din pc's sundhed: dig selv!

Reklamer, sponsorprogrammer og bannere er irriterende, men alle befinder sig trods alt på den "rigtige" side af moralens gærde. Og du vælger i princippet selv, om du vil høre på deres budskaber eller ej.

Men der findes også en lang række lyssky firmaer, som bruger endnu mindre noble metoder til at tiltrække opmærksomhed og penge. Hvis du vil undgå at blive offer for deres snagen i dine private sager og vaner, kræver det først og fremmest, at du udviser et minimum af omtanke, når du bevæger dig rundt på internettet.

Som udgangspunkt gælder de samme tommelfingerregler på nettet som i resten af verden. Hvis noget lyder for godt til at være sandt, så er det nok løgn! Samtidig kan du roligt regne med, at de fleste sider, der skilter med "utrolige gratis tilbud", har en skjult dagsorden, der fx kan gå ud på at få dig til at installere forskellige småprogrammer, som på ingen tid kan føre dig og din computer i uføre og få din telefonregning til at eksplodere.

Tænk dig derfor om, når du surfer, brug din logiske sans, og vær generelt skeptisk over for de store løfter! Hvis du gør det, kan du roligt kaste dig ud i de utallige digitale glæder, som internettet heldigvis først og fremmest byder på.

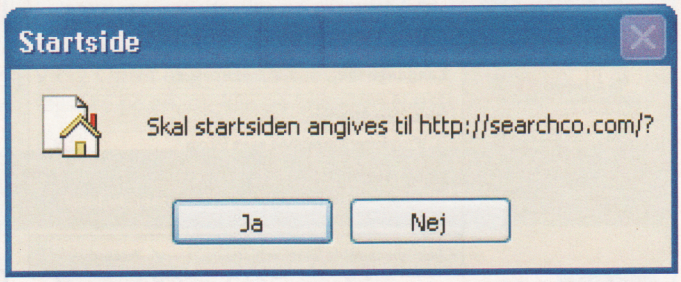
Lad os være din yndlingsside!

I internetverdenen er opmærksomhed lig med succes. Hvis en hjemmeside er et hit, kan den tiltrække annoncer. Og den side, som du besøger alleroftest, er din startside, som dukker op, hver gang du åbner *Internet Explorer*.

Derfor kommer du med garanti ud for hjælpsomme netsider, der tilbyder at gøre netop deres side til din startside, uden du behøver at rode med menuen **Funktioner, Internetindstillinger**. Hvis de har samvittighed, sker det som et link på hjemmesiden, og har du lyst til at følge det, er det din egen sag. Andre gange får du blot uden varsel en dialogboks på skærmen, som spørger, om startsiden skal angives til dette eller hint. Svaret er naturligvis et rungende "Nej!"

Dette fænomen kaldes browser-kidnapning og handler dels om at sikre annoncekroner, dels om at give den pågældende tjeneste et forspring frem for konkurrenterne. I nogle tilfælde kan kidnapningen også skyldes et lille program, som du har fået med, da du besøgte en hjemmeside.

De kan heldigvis fjernes med *Ad-aware*.



Her prøver søgetjenesten Searchco.com at få et forspring ved at kidnappe Internet Explorers startside. Det skal de ikke have lov til. Microsoft gør i øvrigt det samme ved at gøre sin egen hjemmeside til din startside, når du installerer browseren.

Vi har et lille program til dig!

På nogle hjemmesider med "privat" eller "voksent" indhold kan du komme ud for pludselig at blive spurgt, om du vil downloade eller sågar installere et program. I mange tilfælde behøver du ikke engang at klikke på noget for at blive påduttet installationen, den dukker blot op. Her er der grund til at slå bak med det samme, klikke **Annuller** og lukke programvinduet i en fart. Når den slags beskeder dukker op spontant, er påskuddet i reglen, at det er et "hjælpeprogram", som skal gøre det muligt at hente billeder, programmer, eller hvad det nu er, du har ledt efter. Eller en "accelerator", som skal gøre dit modem hurtigere. Programmerne er i nogle tilfælde komplet unødvendige, og i alle tilfælde er det egentlige formål at trække penge ud af dig.

Bag de tillokkende titler gemmer sig nemlig ofte et opkaldsprogram, som erstatter opkaldsprogrammet til dit modem og ringer til en computer i et fjernt land i stedet for at bruge din normale internetudbyder. Før du ser dig om, kan telefonregningen være vokset til astronomiske højder.

Den gode nyhed for ca. halvdelen af os er, at sådanne "tropedialere" kun kan ramme dig, hvis du bruger modem eller ISDN. Har du ADSL eller kabelmodem, sker din internetforbindelse altid via din internetudbyder, den kan ikke stjæles og omdirigeres af luskede programmer.

Jamen jeg er jo uskyldig!

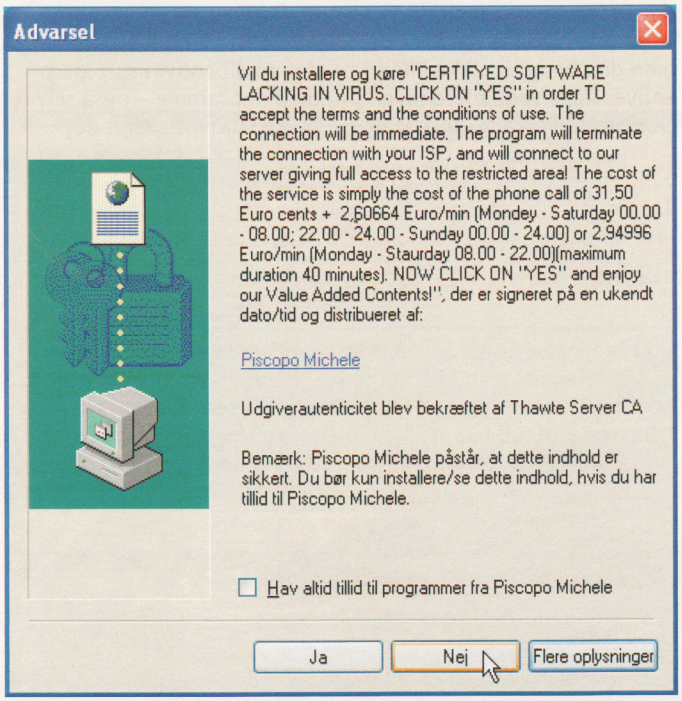
Total uskyld og ren samvittighed er ikke altid nok til at undgå problemer. Især ikke hvis du har ADSL eller kabelmodem. Faktisk kan du komme alvorligt i fedtefadet og blive stemplet som slibrig spammer uden at have gjort noget som helst – ud over at have været så letsindig at oprette adgang til nettet, selvfølgelig.

Du kan således opleve at få en ubehagelig besked fra dit postprogram om, at du ikke kan sende mail, fordi din IP-adresse er røget på den sorte liste hos en organisation, du aldrig havde hørt om.

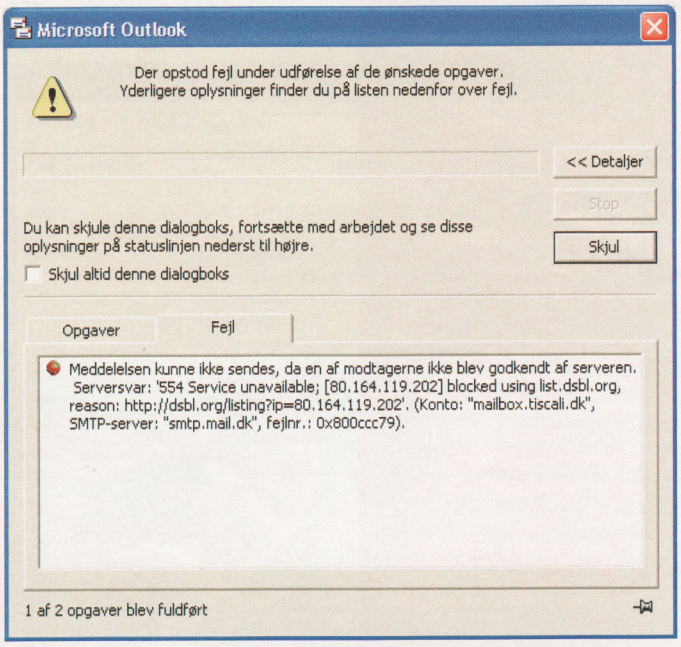
Hvis du er helt sikker på, at du er uskyldig, og at du ikke "kom til" at sende 500.000 reklamebreve ud til tilfældige modtagere tidligere på dagen ved et uheld, kan det godt betale sig hurtigt at ringe til din internetudbyder og forklare dem situationen. Hvis de ikke kan se noget galt ved dit abonnement, er forklaringen sandsynligvis, at dit internetabonnement er af typen med såkaldt dynamisk IP, altså hvor pc'en får tildelt en tilfældig netadresse, når du logger på.

Hvis det er tilfældet, kan en anden kunde have haft samme nummer på et tidligere tidspunkt og brugt det til at sende spam ud.

Den nemmeste løsning er ganske enkelt at tage den med ro, slukke for pc'en og prøve igen senere – og håbe på, at den adresse, du får tildelt tilfældigt næste gang, ikke har tilhørt en spammer.



Hov, hvad er det for et program, de vil have mig til at installere? Hvis du siger "Ja" til dette her, installerer du et nyt opkaldsprogram, som ringer op til internettet for 20 kroner i minuttet. Med andre ord: brug din sunde fornuft, når du bevæger dig rundt på nettet (især hvis du besøger sider med letpåklædte mennesker). Luk vinduet, og skynd dig væk fra hjemmesiden!



Hvis din pc får en tilfældig netadresse, når du logger på, kan du risikere helt uforvarende at blive kaldt spammer uden grund, fordi en anden og mere skrupelløs netforretningsmand har udsendt spam fra samme netadresse som den, du benytter. Organisationen DSBL.org fører jævnligt opdaterede adresselister over mistænkte spammere. På adressen www.dsbl.org kan du således se, om din mailadresse eller dit IP-nummer er røget på listen, og det måske er derfor, du bliver blokeret, når du forsøger at sende mails hjemme fra din pc.

2

TRUSLER MED POSTEN

E-mail er den mest populære anvendelse af internettet. Selv den mest teknologiforskrækkede kan se ideen i at kunne sende og modtage beskeder gratis fra hele verden på få sekunder. Derfor er det næppe overraskende, at e-mail også er blevet populært hos de mørkere kræfter på nettet. Halvdelen af den e-mail, der sendes via internet, er såkaldt spam: uønskede reklamer for tvivlsomme produkter. Dertil kommer tusindvis af virus, der spredes via mail og lægger millioner af computere ned på få timer. Og så er der stadig plads til deciderede svindelnumre, hvor godtroende mennesker narres til at sende penge til den anden side af kloden under løfter om at få "investeringen" mangefold igen. Ikke sært, hvis det nogle gange kan være svært at finde brevet fra moster Anna blandt alle de uønskede beskeder. I dette afsnit får du både værktøjet til at blive fri for uønskede beskeder og farlige pc-virus.

Her er truslerne

Elektronisk post indeholder sin helt egen verden af trusler. E-mails er den største smittespreder for virus. Nogle af dem kan undgås med almindelig sund fornuft, mens andre udnytter fejl i Windows og mailprogrammet Outlook og angriber uden varsel. Mindre farlige, men langt mere irriterende, er mails, som har til formål at narre penge ud af dig: spam og bondefanger-mails. Og problemet er voksende.

Fri for virus og orme i din pc

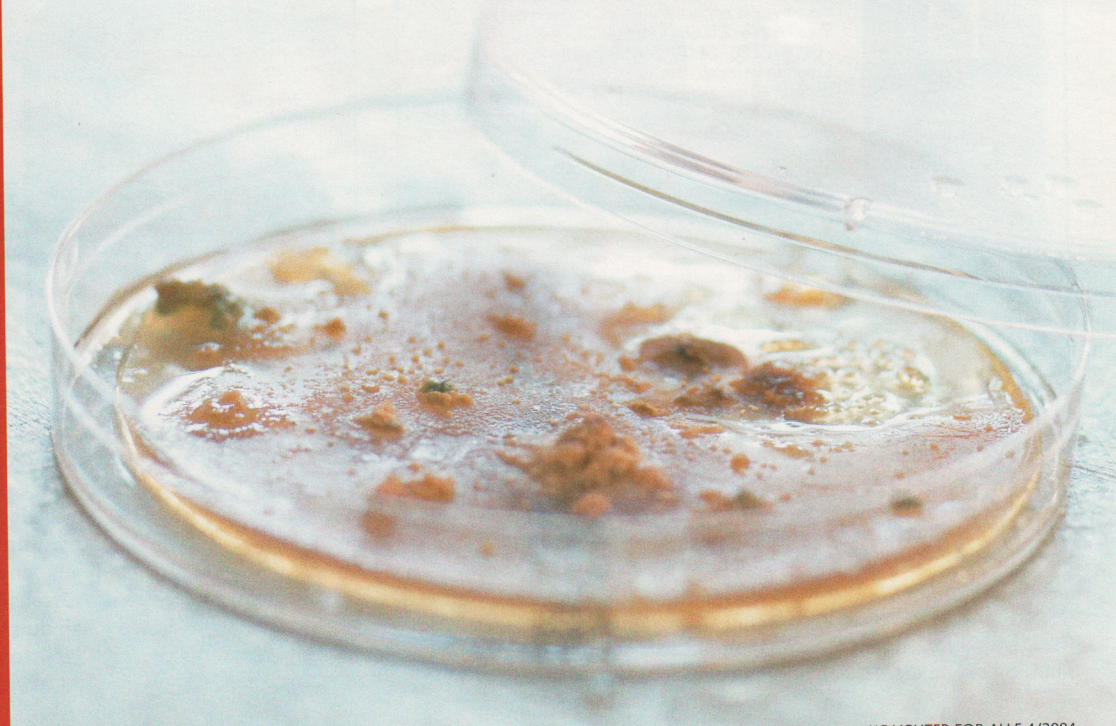
Virus er et problem, som ikke skal ignoreres. Heldigvis er der en gratis kur: AVG Antivirus 6.0

Computervirus er desværre ikke kun noget, der sker for de andre. Uanset om du klæber diskette- og cd-drev til med tape, er pc'en sårbar for angreb, lige så snart du modtager en e-mail. De fleste virus spredes nemlig via e-mail, som sendes fra andre angrebne computere. Og de mest nævenyttige af de digitale ubehageligheder behøver du ikke engang læse for at blive smittet.

"Jamen jeg har jo lige installeret et firewall-program, så nu er jeg vel beskyttet?", spørger du. Desværre nej, en firewall kan holde ubudne gæster ude, men den beskytter ikke imod enhver slags vedhæftede filer. Dørmanden på diskoteket tjekker jo heller ikke alle gæsterne for våben. Og hvad værre er: Hvis du får en virus af typen "trojansk hest" pr. e-mail, kan den bryde firewallen ned indefra og åbne døren for hackere.

Løsningen er at anskaffe et godt antivirusprogram. Og et godt program vil sige et, der opdateres ofte og automatisk kan hente nye virusdefinitioner via internettet. For der kommer nye virustyper hele tiden. Og takket være internettet kan de spredes til hele verden i løbet af få timer eller i heldigste fald få dage.

Derfor er det vigtigt at opdatere dit antivirusprogram med det samme – også selv om du lige har installeret det.

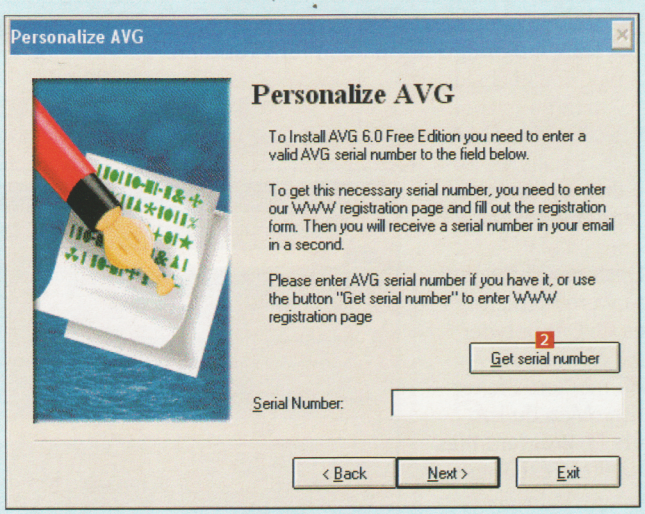


Sådan bruger du AVG Anti-Virus 6.0

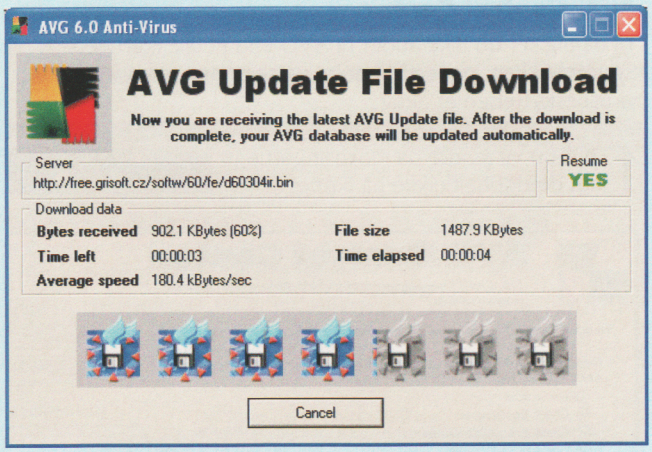
AVG er noget så sjældent som et godt og gratis antivirusprogram, der, blandt mange andre funktioner, kan indstilles til automatisk at foretage periodiske skanninger af din pc for at sikre, at alting er, som det bør være.

Let installation af AVG

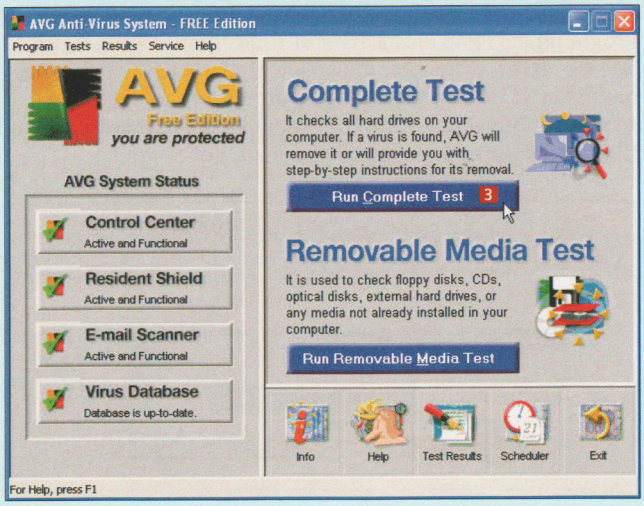
1 Det første der sker, når du installerer *AVG Anti-Virus 6.0* fra cd'en, er, at din browser åbner med producentens hjemmeside, hvor du kan registrere programmet og dermed få det serienummer, du skal bruge under resten af installationen. Udfyld formularen, og tryk på **Continue** 1.



2 Under installationen bliver du herefter bedt om at indtaste et serienummer. Indtast eller indsæt det serienummer, du lige har fået pr. e-mail, i feltet **Serial Number** 2, så er programmet registreret og klar til brug.

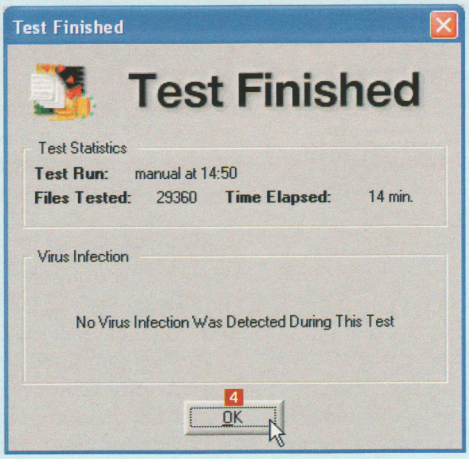


3 Som sidste punkt i installationen foreslår programmet at hente den nyeste virusdatabase via internet. Dette er meget vigtigt, da der løbende kommer en række nye virus til. Alt efter din netforbindelse kan det tage et par minutter.



4 Herefter åbnes programmet *AVG 6.0 for Windows*. Her har du adgang til samtlige programmets funktioner og indstillinger. En af de vigtigste er en komplet skanning. For at starte den klikker du på knappen **Run Complete Test** 3, så skannes hele harddiskens indhold for virus. Det kan dog tage et godt stykke tid, så masser af tålmodighed er påkrævet.

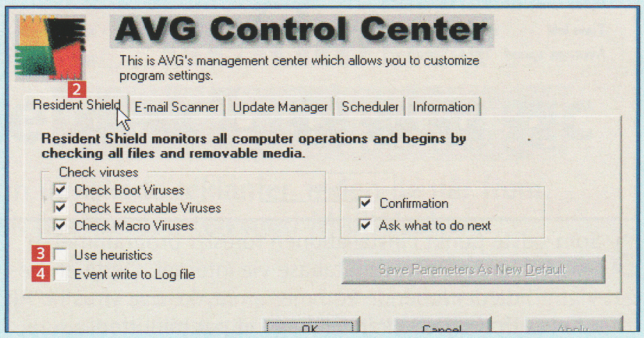
5 Når skanningen er afsluttet, forhåbentlig uden nogen grimme overraskelser, kan du afslutte testen med et klik på **OK** 4 og lukke programmet, indtil du får brug for det igen. Din pc er nu effektivt beskyttet mod alle kendte typer virus på det tidspunkt, skanningen blev gennemført.



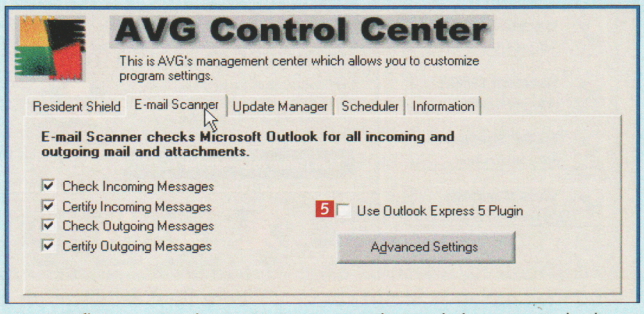
AVG Control Center

Til daglig ser du ikke andet til *AVG* end et lille ikon nede i Systembakken, nederst til højre på skærmen, som viser, at virusbeskyttelsen er aktiv.

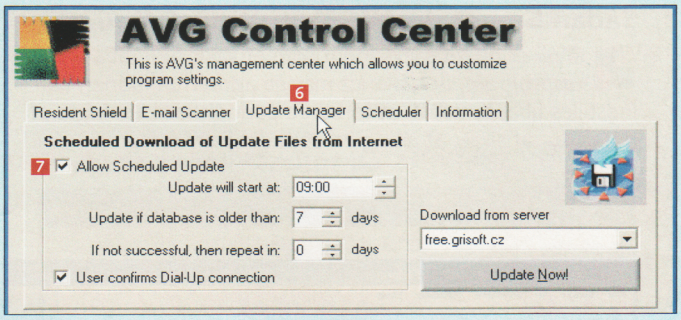
1 Hvis du vil ændre på indstillingerne, kan du dobbeltklikke på ikonet 1.



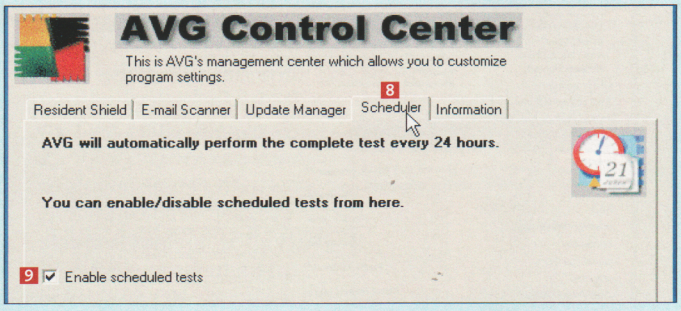
2 På fanen **Resident Shield** 2 kan du bestemme, præcis hvilke typer virus der skal tjekkes for under skanningen. Programmets egne indstillinger er sund fornuft. Hvis du vil føle dig ekstra sikker, kan du vælge at markere i felterne **Use heuristics** 3, som lader *AVG* lede efter programmer, som ikke er kendte virus – men som ligner – og **Event write to Log file** 4, som opretter en logbog over alt, der er gjort.



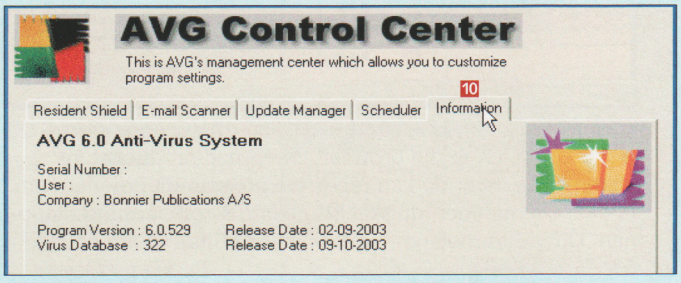
3 De fleste virus kommer pr. e-mail. Med de viste indstillinger bliver både indkommende og afsendte mails tjekket for virus og mærket med en kvittering for kontrollen. Medmindre du bruger *Outlook Express 5*, skal du til gengæld ikke markere feltet **Use Outlook Express 5 Plugin** 5.



4 Det er livsvigtigt at opdatere dit antivirusprogram ofte. På fanen **Update Manager** 6 indstiller du, hvordan og hvornår *AVG Anti-Virus* henter nye virusdefinitioner over internettet. Det letteste er at indstille programmet til selv at hente opdateringerne 7 – helst på et tidspunkt, hvor du normalt har pc'en tændt.

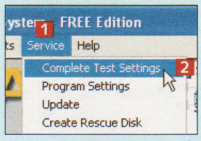


5 *AVG Anti-Virus* udfører en test af hele pc'en en gang i døgnet. På fanen **Scheduler** 8 kan du slå den til og fra 9. Vil du ændre indstillinger, kan det ske i *AVG 6.0 for Windows*.



6 På fanen **Information** 10 finder du blandt andet programversionen og udgivelsesdatoen for viruslisten.

Indstillinger for fuld skanning



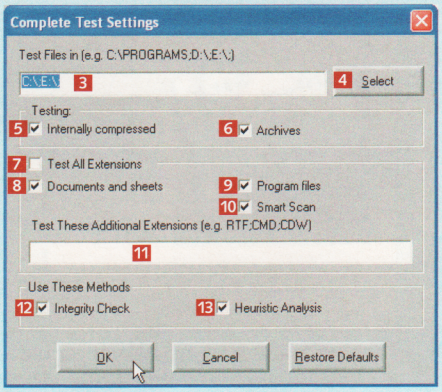
1 I menuen **Service** 1, **Complete Test Settings** 2 kan du vælge, hvor, hvordan og hvor meget der skal skannes, når *AVG* foretager den daglige komplette skanning af pc'en.

2 I feltet **Test Files in...** 3 kan du se, hvilke drev og mapper der skannes. Hvis du vil ændre på listen, er det lettest at klikke på knappen **Select** 4 og udvælge dem.

Virusfiler kan gemme sig i pakkede filer. Derfor er det vigtigt at lade AVG skanne disse også, og der skal så være markering i felterne **Internally compressed** 5 og **Archives** 6. Det betyder dog, at skanning tager lidt længere tid.

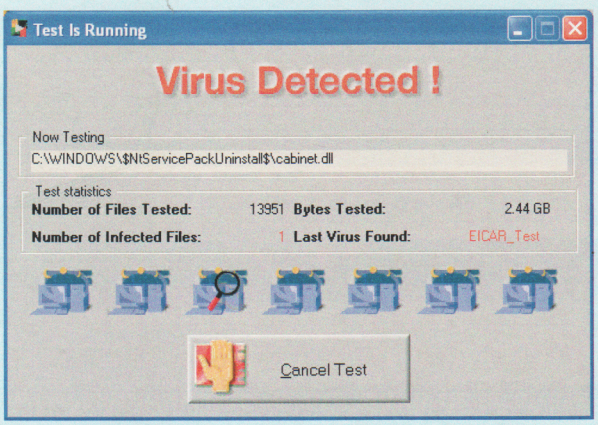
Hvis du vil være 100 procent sikker, kan du markere i feltet **Test All Extensions** 7. Så skannes alt på disken. Men du kan nøjes med at markere i **Documents and sheets** 8, **Program files** 9 og **Smart Scan** 10. Nye filtyper kan tilføjes i feltet **Test These Additional Extensions** 11.

Endelig kan du bestemme, hvilken type skanning der foretages. **Integrity Check** 12 undersøger filerne for programkode, der tilhører kendte computervirus. **Heuristic Analysis** 13 finder desuden programkode med "viruslignende opførsel" – altså programmer, som måske kan være en ny, ukendt virustype.

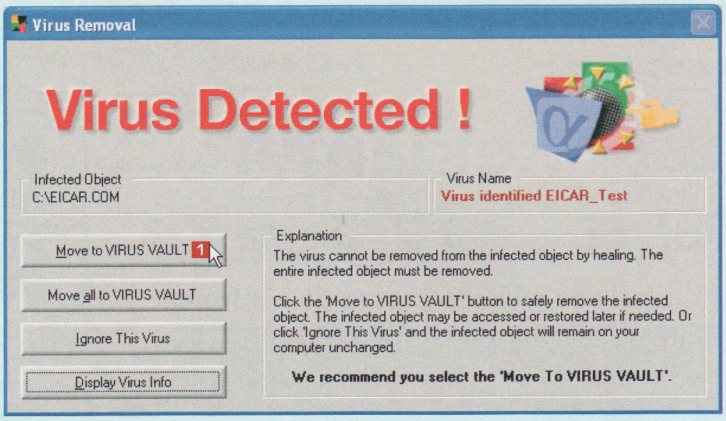


Når uheldet er ude

Men hvad nu, hvis eller når dine værste anelser bliver bekræftet, og din kære pc er smittet med virus? Her ser du, hvad der sker, hvis *AVG* støder på en virus på harddisken.



1 Her er en computervirus blevet opdaget og identificeret undervejs i harddiskskanningen.

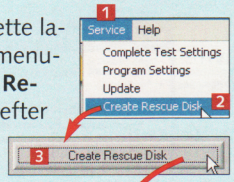


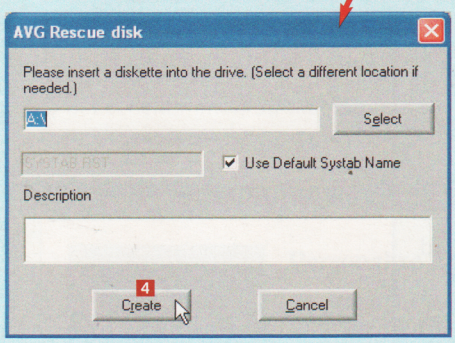
2 Hvis det kan lade sig gøre, vil *AVG* prøve at fjerne viruskoden fra det ramte program. I dette tilfælde er der dog ikke noget at gøre, og anbefalingen er at flytte det mistænkte program til *AVG*'s sikrede "bankboks". Klik på **Move to VIRUS VAULT** 1.

Lav en sikkerhedsdiskette

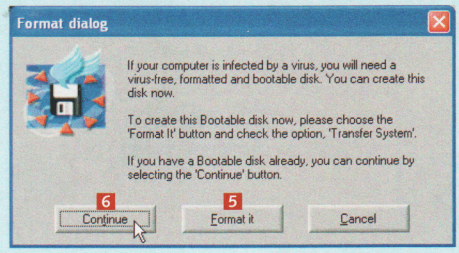
Hvis uheldet alligevel er ude, og maskinen en morgen er for syg til at starte, er det godt at have en diskette, som kan genetablere de livsnødvendige systemfiler og samtidig give et "rent" udgangspunkt for en virusskanning.

1 En sikkerhedsdiskette laves ved at vælge menuen **Service** 1, **Create Rescue Disk** 2. Klik derefter på knappen **Create Rescue Disk** 3.



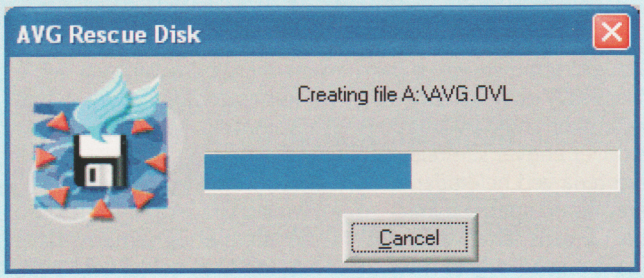


2 Nu skal du indsætte en diskette i diskdrevet. Gør det, og klik på **Create** 4.

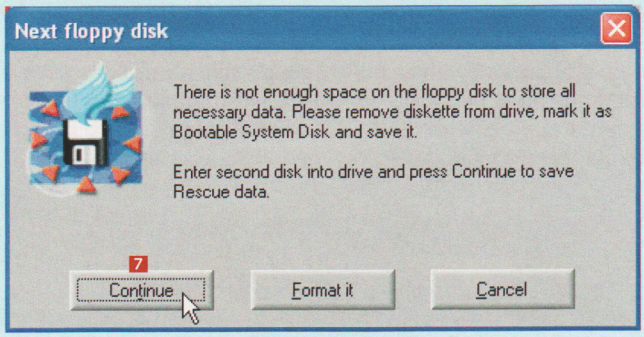


3 Hvis disketten ikke allerede er formateret, kan du gøre det ved at klikke på knappen **Format it** 5. Hvis den er, kan du klikke **Continue** 6.

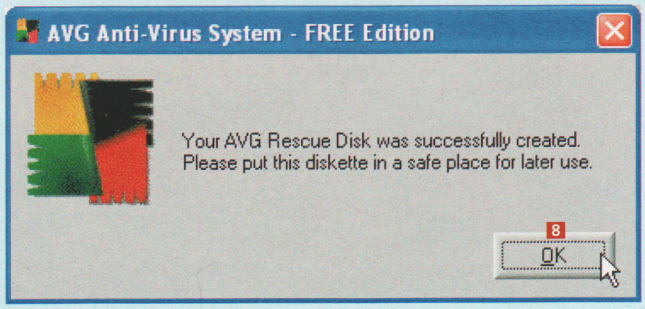
4 Nu kopieres filerne til sikkerhedsdisketten. På den blå barre kan du se, hvor langt computeren er nået med kopieringen. Vær forberedt på, at det kan tage et stykke tid.



5 Filerne fylder så meget, at der skal to disketter til for at få plads til det hele. Indsæt en ny formateret diskette, og klik på **Continue** 7. Programmet sørger for at dele filerne op på disketterne.



6 Nu mangler du blot at gemme dine nye sikkerhedsdisketter – og så ellers håbe på, at du aldrig får brug for dem. Afslut ved at klikke på **OK** 8.



Sæt "Reklamer nej tak" på din pc

Fjern uønskede reklamer, inden de når frem. Vask postkassen ren med MailWasher.

"Pling" – en ny mail er dumpet ind i din mailboks. Måske er det et brev fra en af vennerne eller den rapport, som du har ventet på. Nej, det er tilsyneladende en reklame af en slags. En akademisk organisation, du aldrig har hørt om, tilbyder dig et eksamensbevis, uden at du behøver at gå på universitetet. Det koster blot 500 dollars. Du har med andre ord fået endnu en spam-mail.

Navnet spam stammer fra en klassisk Monty Python-sketch, hvor en flok vikinger overdøver enhver samtale på et cafeteria ved hele tiden at synge "spam-spam-spam-spam". Præcis sådan føles det at få sin mailboks fyldt med spam. Før du ved af det, drukner alle meningsfulde mails i de uønskede "tilbud", som du skal bruge dyrebar båndbredde på at hente fra internettet og derefter endnu mere dyrebar tid på at slette.

Programmet *MailWasher* kan ikke få spam til at holde op med at eksistere, men det kan i hvert fald løse de to førnævnte problemer ved at slette spam-mailene, inden de hentes fra internettet.

MailWasher fungerer ved at søge på typiske kendetegn for spam-mails. For eksempel at de sendes til en hemmelig liste af modtagere. Du kan desuden oprette en liste over venner og uvenner, hvis mails skal henholdsvis godkendes og slettes automatisk.

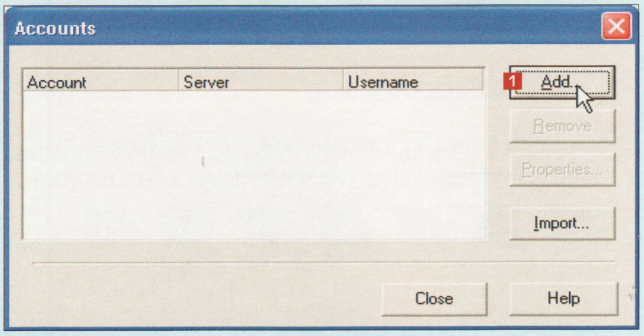
Betal, hvad du ønsker

Hvis du vil være fri for reklamebanneret og samtidig have adgang til at tjekke flere postkonti og Hotmail, er du nødt til at betale for programmet. Standardprisen er $20, men hvis du synes, at prisen er forkert, er programmøren til at forhandle med. Vælg din pris – ned til $3, eller op til $100!

Sådan bruger du MailWasher Free 2.0

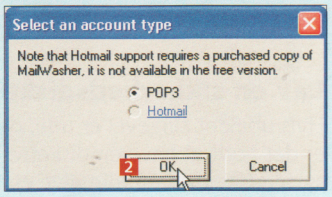
Med *MailWasher* kan du tjekke dine mails og tage livet af de uønskede reklamer, før de når din brevkasse.

Forbered MailWasher på arbejdet

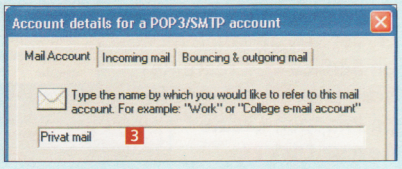


1 Det allerførste, du skal gøre, er at indstille programmet til at tjekke din mailkonto. Klik på **Add** 1.

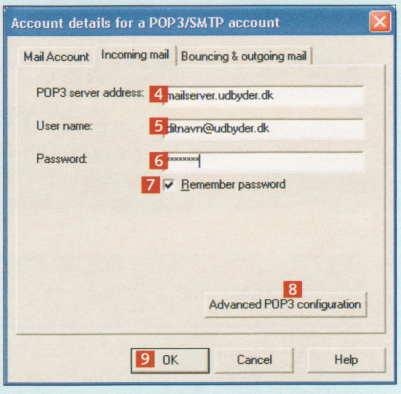
2 Den gratis udgave af *MailWasher* kan kun læse almindelige POP3-mails. Hvis du vil have tjekket en Hotmail-adresse, er du nødt til at købe programmet (se boks). Klik **OK** 2.



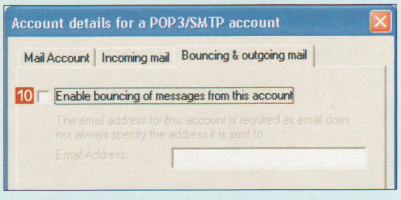
3 Giv kontoen et beskrivende navn 3, så du efterfølgende selv kan finde rundt i dine mapper, og klik på **OK**.



4 Nu skal du indtaste navnet på postserveren (**POP3 server address**) 4, dit brugernavn (**User name**) 5 og din adgangskode til e-mail (**Password**) 6. Klik i **Remember password** 7, hvis du vil slippe for at indtaste adgangskoden igen og igen. Hvis din postserver stiller særlige krav, kan du indtaste flere oplysninger under **Advanced POP3 configuration** 8. Fortsæt med **OK** 9.

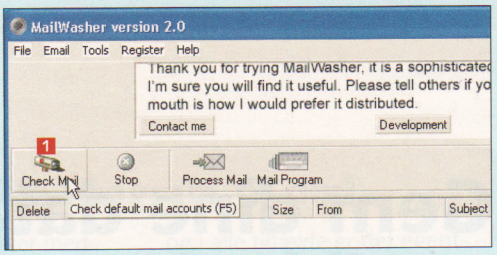


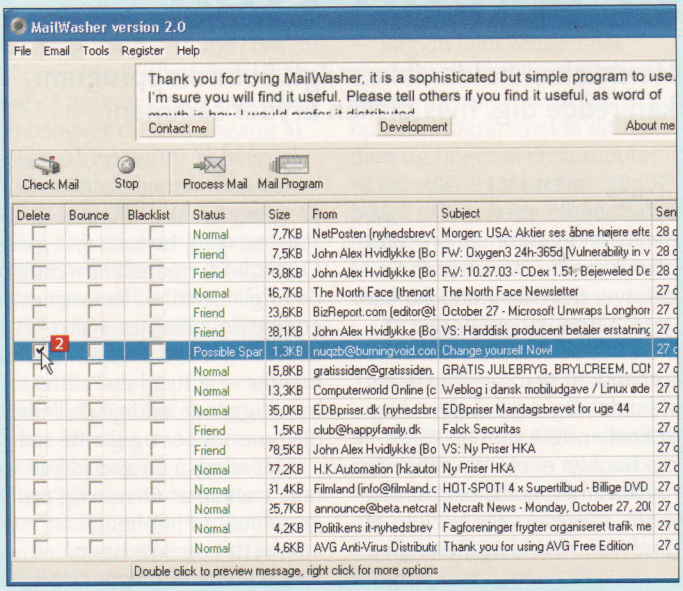
5 Hvis du ønsker det, kan du sende spam-mailene tilbage i hovedet på afsenderen ved at markere i **Enable bouncing of** 10 Ideen er fristende, men spammere gemmer sig i reglen bag falske mailadresser for at undgå præcis dette. Og skulle mailen nå frem alligevel, vil det blot anspore til mere spam. Så drop ulejligheden, og spar internettet for belastningen.



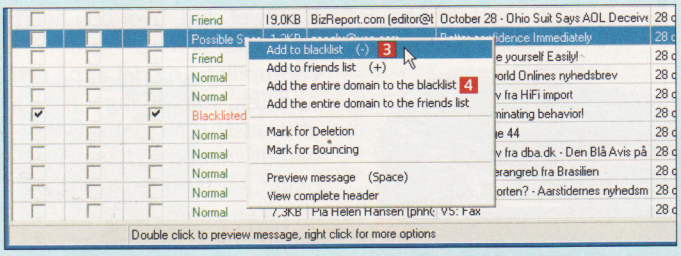
Få hurtigt gang i mailvaskeriet

1 Nu er det tid at sætte programmet på arbejde. Klik på **Check Mail** 1, så hentes emnerne på dine e-mails fra mailserveren.

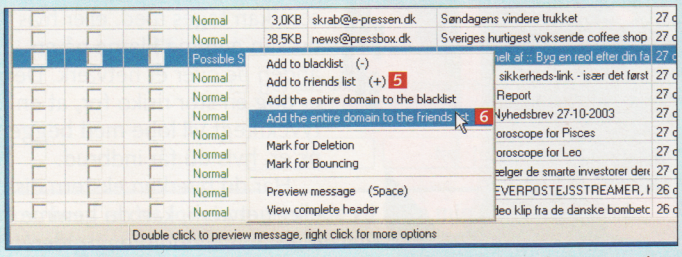




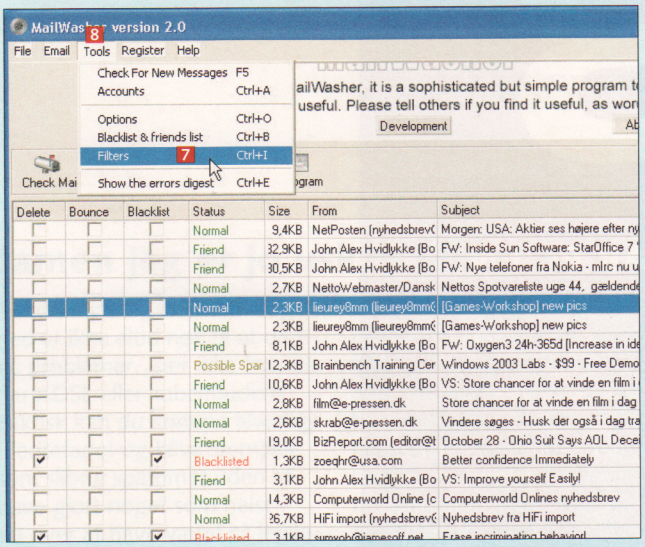
2 Programmet prøver at genkende spam ud fra en række forskellige kendetegn (fx at mailen sendes til en hemmelig liste af modtagere). Klik i feltet **Delete** 2 for at slette mailen.



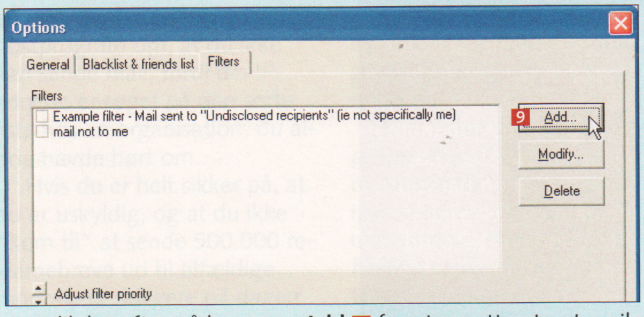
3 Når du har fundet en spammer, kan du slippe helt for at få mail fra samme afsender ved at sortliste ham. Højreklik på spam-mailen, og vælg **Add to blacklist** 3. Hvis du mistænker udbyderen for at lægge hus til spam frivilligt, kan du udelukke alt fra dén kant med **Add the entire domain to the blacklist** 4.



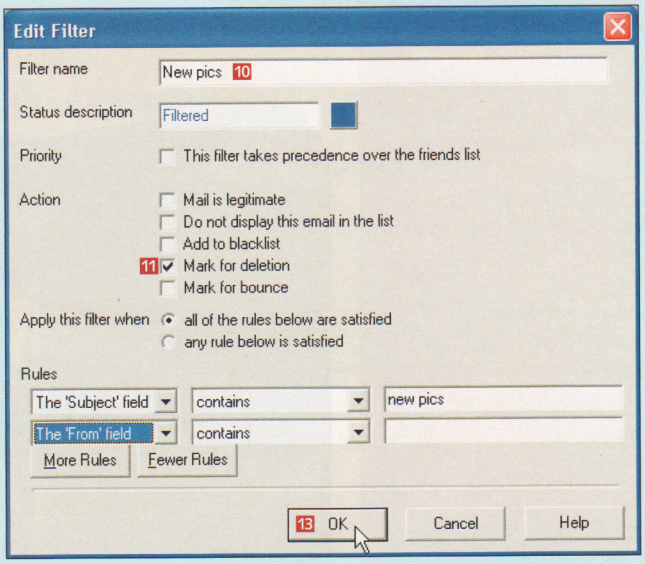
4 Omvendt kan uskyldige nyhedsmails komme under mistanke. Dem kan du rense ved at mærke dem som "venner": **Add to friends list** 5 eller **Add the entire domain to the friends list** 6.



5 Du kan også vælge at lære *MailWasher* en række nye tricks ved at klikke på **Filters** 7 i menuen **Tools** 8.



6 Klik herefter på knappen **Add** 9 for at oprette et nyt mailfilter, programmet kan arbejde med.



7 Postlister er ofte udsat for spam-meddelelser, der typisk fx lover spændende nye billeder. Her har vi valgt, at mails, hvor emnet (**Subject**), der indeholder ordene "New pics" 10, automatisk skal slettes, når de ankommer (**Mark for deletion**) 11. Med knappen **More Rules** 12 kan man tilføje flere betingelser, enten for at gøre filteret mere avanceret eller lade det fange flere slags spam på én gang. Klik på **OK** 13 to gange for at gøre filteret færdigt og tage det i brug.

3

NÅR PC'EN FEJLER

Din pc er et stykke elektronisk værktøj, og som alle andre stykker elektronik kan skidtet gå i stykker. Men hvor det er rimelig enkelt at udskifte en defekt boremaskine og et sammenbrændt fjernsyn, så kan et computersammenbrud være en anderledes katastrofal og dyrebar sag, især hvis du ikke har sørget for at sikre de vigtigste af dine data, før pc'en opgiver ævred. Men selv om du aldrig kan sikre dig helt, så kan du forhindre de værste katastrofer ved dels at sørge for en backup af dine data og dels ved at udnytte Windows XP's indbyggede mulighed for at gendanne computerens indstillinger, når uheldet har været ude. Se her hvordan.

Her er truslerne

Ikke alle fejl skyldes menneskelig nedrighed. Hardwaren og programmerne på din pc kan sagtens skabe problemer i sig selv. Hvad stiller du fx op den dag, da harddisken holder op med at fungere? Eller hvor Windows går i baglås, fordi et program, som du installerede, har opført sig forkert og lavet rod i registreringsdatabasen?

Gem dine data et sikkert sted

Harddisken holder ikke evigt. Et backupprogram kan redde dig, hvis disken bryder sammen.

"Rigtige mænd tager ikke backup – men de græder ofte." Sådan lyder et gammelt ordsprog blandt nørder. Men sådan behøver det ikke være. Du kan spare tårer og besvær ved at bruge et backupprogram til automatisk at gemme dine vigtigste data. Og det behøver ikke at koste noget som helst. *Ceren Backup* er et udmærket og fuldkommen gratis backupprogram, som kan tage backup af dine filer med faste intervaller.

Hvilke filer skal jeg tage backup af?

Der er ingen grund til at tage backup af alle filer på harddisken. Windows og alle dine programmer skal alligevel installeres igen, hvis det går galt. Og til det formål skal du bruge de originale cd'er. Det vigtigste er dine dokumenter, hvilket for de fleste vil sige mappen **Dokumenter** – og hvad du måtte have liggende af digitalbilleder, hjemmevideoer og gemte spil.

Det er også en god idé at tage backup af drivere og programmer, du har hentet fra internettet og ikke har på cd eller diskette. Så slipper du for at skulle finde dem igen.

Hvor skal jeg gemme mine backupfiler?

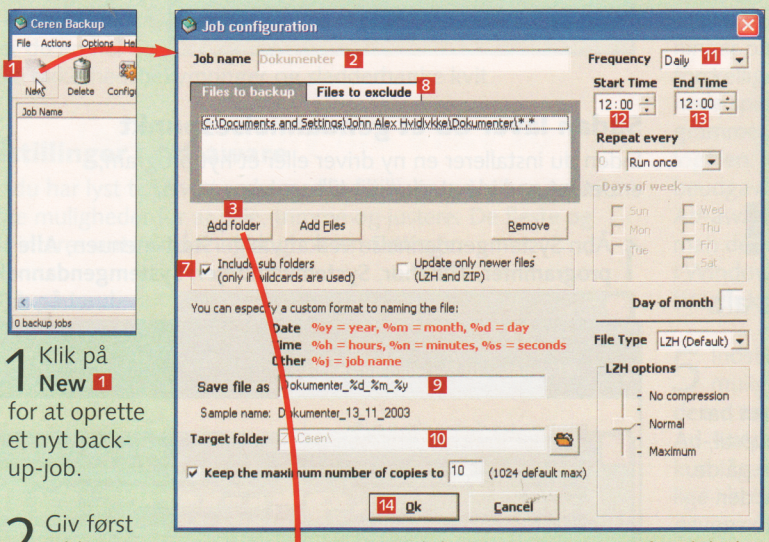
Der er ét sted, hvor du i hvert fald aldrig skal gemme dine backupfiler – og det er på den harddisk, som du tager backup af! Uanset om tabet skyldes harddisknedbrud, tyveri eller brand, mister du med garanti alt på én gang.

Hvis du har to forskellige harddiske (og ikke blot to partitioner på samme harddisk), kan du sikre dig mod disknedbrud ved at gemme dataene på den anden disk. Bedre er det dog, hvis du har en ekstern disk, som kan tages med, eller hvis du kan gemme filerne på en anden pc over et netværk. Der er dog en stor risiko for, at en tyveknægt vil løbe med begge pc'er, hvis du får indbrud.

Har du hverken ekstern disk eller netværk, kan du gemme filerne på harddisken og derefter brænde dem på en cd, som du gemmer et sikkert sted (på arbejdet, i sommerhuset eller hos din bedste ven).

Sådan bruger du Ceren Backup

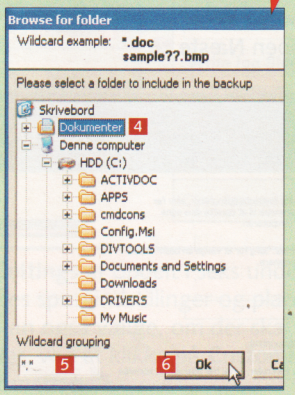
For at lave en backup opretter du først en såkaldt opgave, hvor du vælger, hvilke filer der skal tages backup af hvordan og hvor ofte.



1 Klik på **New** 1 for at oprette et nyt backup-job.

2 Giv først jobbet en titel i feltet **Job name** 2.

3 Klik på knappen **Add folder** 3 for at udpege den eller de mapper, der skal tages backup fra.



4 Klik på den mappe, som du vil have backup af. Et godt valg er mappen **Dokumenter** 4.

5 I feltet **Wildcard grouping** 5 kan du bestemme, hvilke typer der skal med i backuppen. *.* betyder alle filer. Hvis du vil nøjes med Word-dokumenter, skal du skrive "*.doc" i feltet. Klik på **Ok** 6.

6 Du har nu valgt mappen **Dokumenter**, men vi skal have alle undermapper med også. Klik i feltet **Include sub folders** 7.

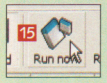
7 Hvis dokumentmappen også indeholder filer, som du ikke ønsker at få med i backuppen (for eksempel en stor sampling af MP3'er), kan du klikke på **Files to Exclude** 8 og fravælge dem.

8 Hele backuppen gemmes som én komprimeret fil. Nu skal den navngives. Det sker i feltet **Save file as** 9. Ud over teksten (fx "Dokumenter") kan du indsætte tidspunktet som år, måned, dag, timetal, minuttal og sekunder.

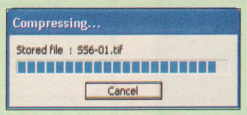
9 Vælg en mappe, som backupfilen skal gemmes i. Det sker i feltet **Target folder** 10. Mappen skal være oprettet i forvejen, for at du kan bruge den.

10 Bestem nu, hvor ofte der skal tages backup. I feltet **Frequency** 11 kan du vælge **Daily** (dagligt), **Weekly** (ugentligt) eller **Monthly** (månedligt), mens felterne **Start Time** 12 og **End Time** 13 bestemmer, hvornår på dagen backuppen skal starte. Er pc'en ikke tændt på starttidspunktet, går backuppen i gang, så snart du åbner Windows, medmindre sluttidspunktet er overskredet også. Klik på **Ok** 14.

11 Hvis du vil lave en backup med det samme, kan du klikke på **Run now** 15.



12 Nu gemmes alle filer i backupsættet i en komprimeret fil.

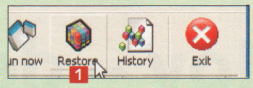


13 Når backuppen er færdig, er der dukket en ny fil op i mappen 16.

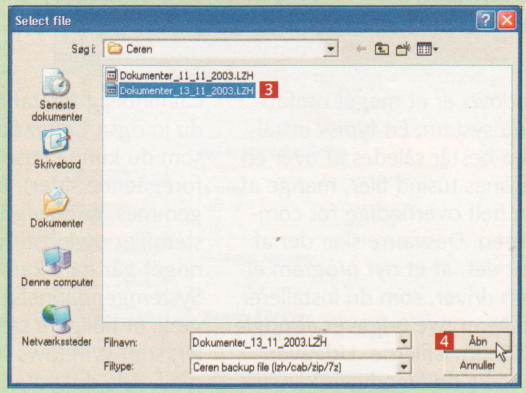
Sådan får du dine filer igen

Pludselig en dag er uheldet ude! Harddisken giver en fæl skrabende lyd fra sig, eller junior har hygget sig med **Formater**-kommandoen. Godt, at du havde en backup! Find i ro og mag din sikkerhedskopi frem, og start *Ceren Backup*.

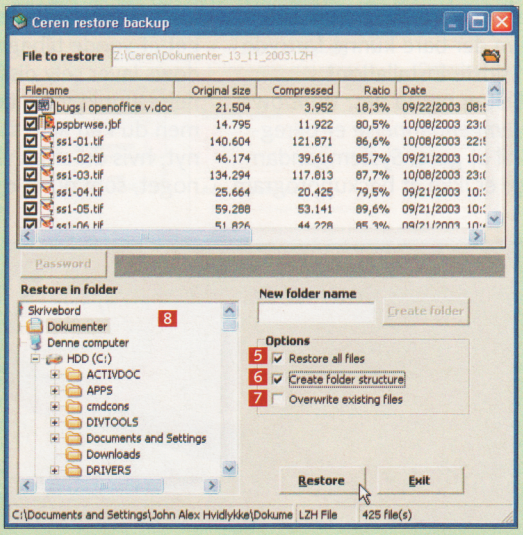
1 Klik på **Restore**-knappen 1 for at starte gendannelsen.



2 Nu skal du finde backupfilerne. Klik på mappeikonet 2.



3 Nu skulle du gerne kunne finde backupfilerne uden problemer – for du lagde dem vel ikke på den harddisk, der gik ned? Vælg nu den backup, som du vil have 3, og klik på **Åbn** 4.



4 Nu kan du udvælge filerne i det øverste vindue. Hvis du vil have fat i det hele, skal du markere i **Restore all files** 5. Det er også en god idé at markere **Create folder structure** 6, sådan at filerne placeres på samme måde som før. Hvis du har nogle data tilbage på harddisken, bør du til gengæld undgå **Overwrite existing files** 7, som erstatter de eksisterende (og muligvis nyere) filer med dem fra backuppen. Endelig – og vigtigst – vælg, i hvilken mappe hele herligheden skal pakkes ud. Det gør du i vinduet **Restore in folder** 8.

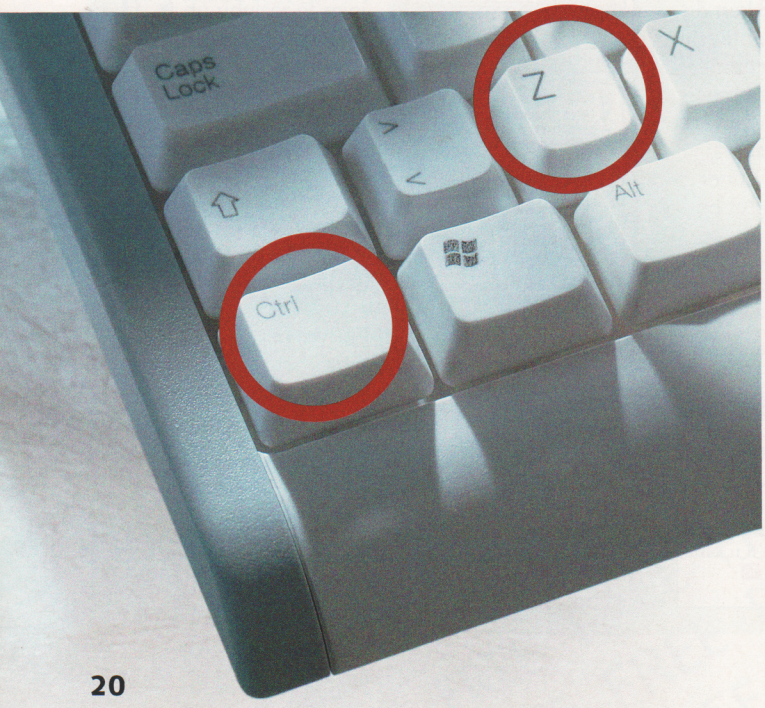
Hov – det ville jeg ikke alligevel!

Systemgendannelse stiller uret tilbage, til da alt var godt – før du begik dine fejl på pc'en.

Windows er et meget omfattende system. En typisk installation består således af over en halv snes tusind filer, mange af dem helt overflødige for computeren. Desværre sker der af og til det, at et nyt program eller en driver, som du installerer, installerer nye udgaver af nogle af Windowsfilerne. Udgaver, som ikke nødvendigvis kan arbejde sammen med alle dine andre filer, hvorefter Windows går i knæ eller begynder at opføre sig underligt. Desværre er det ikke sikkert, at det hjælper at afinstallere programmet. Hvem der bare kunne fortryde den sidste installation!

Det er netop det, *Windows' Systemgendannelse* er beregnet til at gøre. Systemgendannelse er ikke et backupprogram i almindelig forstand (det har du jo også *Ceren Backup* til, som du kunne læse om på de foregående sider). Det, der gemmes, er de vigtigste systemfiler og indstillinger. Hvis noget går galt, kan du med Systemgendannelse rulle tilbage til et tidligere sæt systemfiler, som Windows fungerede med. Alle dokumenter og programmer er uændrede.

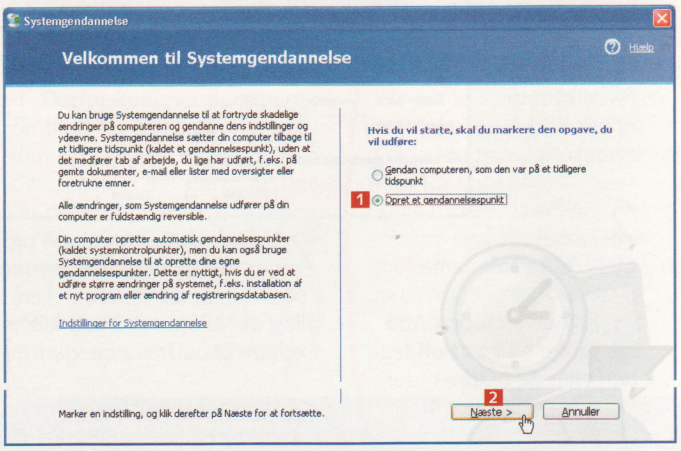
For at kunne stille tiden tilbage er det dog nødvendigt at have lavet et gendannelsespunkt – altså et sæt systemfiler og indstillinger, så man har noget at vende tilbage til. Windows laver selv disse gendannelsespunkter fra tid til anden, men du kan altid selv lave et nyt, hvis du er på vej til at gøre noget, som du er usikker på.



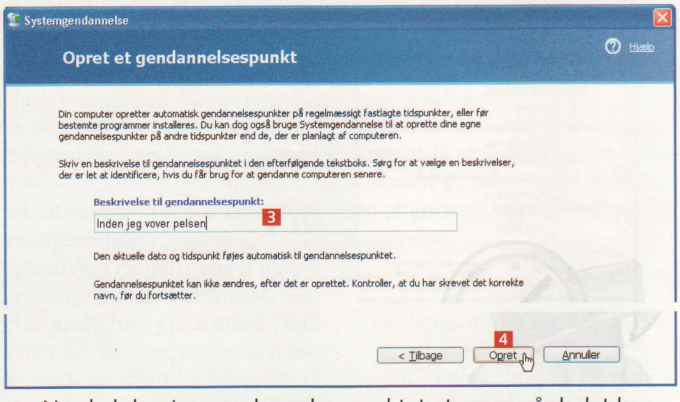
Sådan laver du et gendannelsespunkt

Inden du installerer en ny driver eller et nyt program, er det en god idé at sikre dit tilbagetog.

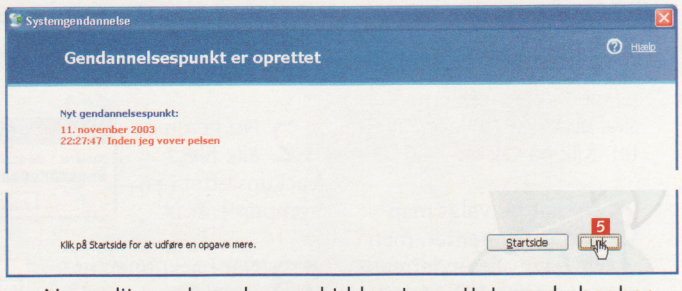
1 Åbn Systemgendannelse ved at vælge **Start**-menuen, **Alle programmer**, **Tilbehør**, **Systemværktøjer**, **Systemgendannelse**.



2 Vælg **Opret et gendannelsespunkt** 1 for at gøre klar til at fejlsikre pc'en, og klik på knappen **Næste** 2.



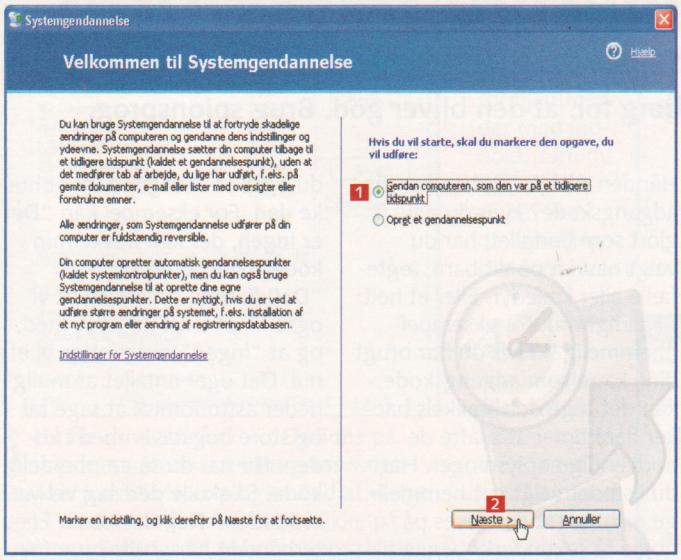
3 Nu skal du give gendannelsespunktet et navn, så du let kan genkende det. Skriv navnet i feltet **Beskrivelse til gendannelsespunkt** 3, og klik herefter på **Opret** 4.



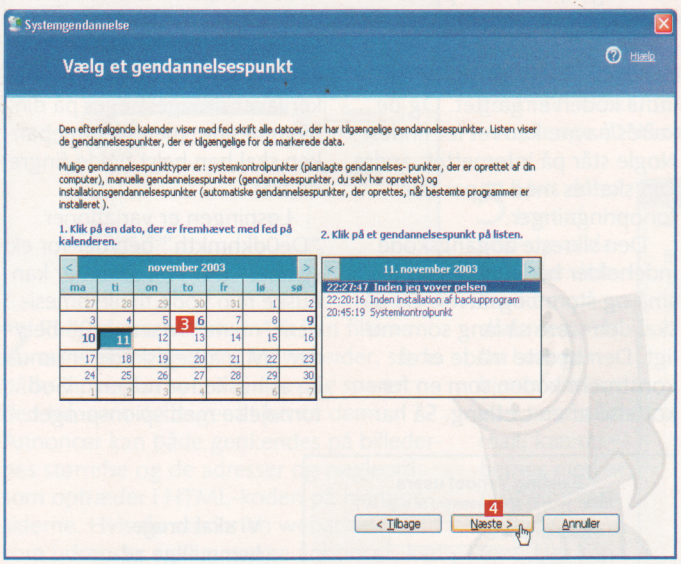
4 Nu er dit gendannelsespunkt blevet oprettet, og du har hermed en god chance for at få Windows på benene igen, hvis et program ikke opfører sig ordentligt. Klik på **Luk** 5.

Sådan bruger du Systemgendannelse

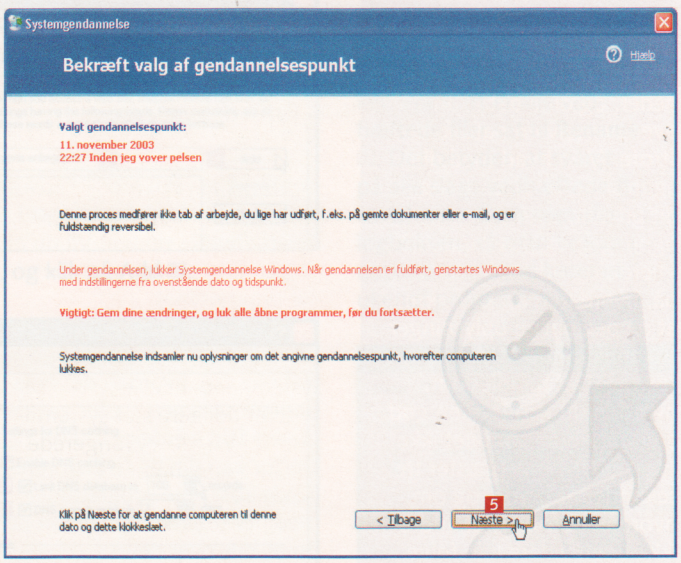
Hvis uheldet er ude, og du har brug for at vende tilbage til tidligere tiders storhed, starter du blot **Systemgendannelse** igen.



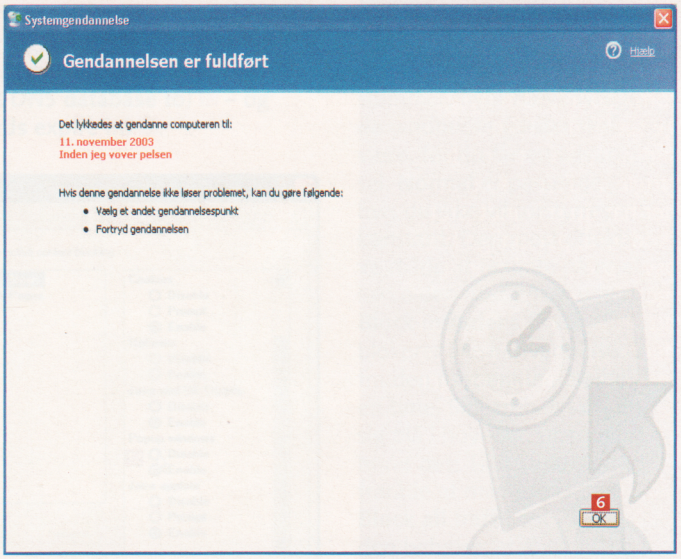
1 Hvis Windows går kold, har du nu heldigvis mulighed for at bruge dine gendannelsespunkter til at vække computeren til live igen, uden at dine livsvigtige data går tabt af den grund. For at gøre det skal du vælge **Gendan computeren, som den var på et tidligere tidspunkt** 1. Det lyder dramatisk, men bare rolig, alle dokumenter bevares alligevel. Klik på **Næste** 2.



2 Nu skal du vælge det gendannelsespunkt, du vil gå "tilbage" til. De dage, som er markeret med fed skrift i kalenderen 3, har ét eller flere gendannelsespunkter, som du kan bruge. Det betaler sig i reglen at vælge det nyeste, men hvis du er usikker på, om problemerne allerede da var opstået, så vælg et ældre gendannelsespunkt. Træf dit valg, og klik på **Næste** 4.



3 Nu får du en sidste påmindelse om, hvad det egentlig er, du er i gang med at gøre – og får med store røde bogstaver endnu en besked om, at dette skam ikke er farligt! Glem nervøsiteten, og gå roligt videre, din pc tager som sagt ikke skade af "indgrebet". Husk dog at lukke dine programmer, da pc'en skal genstartes som led i gendannelsen. Klik på **Næste** 5.



4 Når pc'en er genstartet, modtager du en besked om, at gendannelsen lykkedes. Bemærk, at selv om du lige har "fortrudt" dine seneste installationer, kan også dette fortrydes, og du kan på den måde efterfølgende træde frem og tilbage i tiden mellem andre gendannelsespunkter, hvis resultatet ikke bliver tilfredsstillende i første forsøg. Klik på **OK** 6.

4

PERSONLIG SIKKERHED

Hvis du har fulgt vejledningerne i dette hæfte, er din pc sikret mod hackere virus og andre ubehageligheder, og dine data kan overleve selv en naturkatastrofe. Men hvad med din egen sikkerhed? Er du og dit privatliv sikret mod nysgerrige øjne og posekiggere? I fjerde og sidste del ser vi på, hvordan man kan sikre, at de personlige oplysninger bliver ved med at være personlige. Det handler om, hvordan du kan lave en god adgangskode, som det ikke tager uvelkomne gæster tre sekunder at bryde, og om, hvordan du sikrer, at andre ikke uden videre kan følge dine spor på internettet.

Her er truslerne

Midt i bekymringen for den kære pc's velbefindende må vi ikke glemme din egen sikkerhed. Den personlige computer kommer til at indeholde en mængde informationer om dig, informationer, som nysgerrige sjæle med teknisk indsigt nemt kan aflure den. Nogle af disse informationer har du selv indtastet (kodeord, personlige breve osv.), mens andre er kommet der "af sig selv", når du bruger pc'en. Det gælder fx sporene af de hjemmesider, som du besøger.

Pas godt på dine vigtige passwords

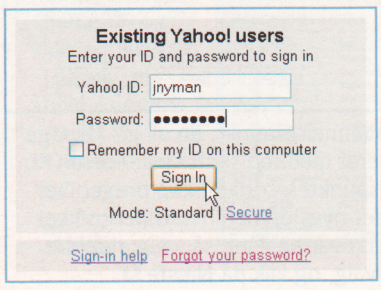
Adgangskoden sikrer dine personlige data. Så sørg for, at den bliver god. Brug spionsprog.

Hånden på hjertet, hvad er din adgangskode? Hvis du har gjort som flertallet, har du valgt navnet på dit barn, ægtefælle eller kæledyr. Eller et helt tilfældigt ord, for eksempel "hemmelig"! Hvis du har brugt dine kære som adgangskode, kan det tage den stakkels hacker flere timer at skaffe de nødvendige oplysninger. Har du i stedet valgt det hemmelige ord, kan koden løses på nogle få sekunder! I begge tilfælde er dine data ikke særlig godt beskyttede.

Når det gælder adgangskoder, er opskriften: Jo længere og mere tilfældigt det kan blive, desto bedre. Hvis ordet står i ordbogen, kan man pudse et hackerprogram med indbygget ordbog på opgaven og simpelt hen lade det prøve sig frem, indtil koden er gættet. Og de kæres navne kan ret let findes. Nogle står på internettet, andre kan skaffes med et par telefonopringninger.

Den sikreste adgangskode indeholder både tal, tegn og små og store bogstaver. Og så skal den være så lang som muligt. Den bedste måde er at konstruere koden som en forkortelse af en sætning. Så har du også en mulighed for at huske den. For eksempel kan "**Der er ingen, der kan huske min kode**" oversættes til "**De0dkhmk**". Bemærk, at vi også fik et stort bogstav med, og at "ingen" oversættes til et nul. Det øger antallet af muligheder astronomisk at tage tal og store bogstaver med i koden. Nu har du så en ubrydelig kode. Så skulle den sag vel være i orden? Nej, desværre. Efterhånden har vi alle brug for flere adgangskoder. En til hjemmebanken, en til internettet, en til pc'en på arbejdet, til nyhedsgrupper, hjemmeside og meget mere. Og det er ikke nogen god idé at bruge samme sikre kode overalt. Hvis blot sikkerheden fejler et enkelt sted, er alle døre pludselig åbne. Og du kan måske leve med, at en hacker laver drengestreger på din hjemmeside, men hjemmebanken skal han helst holde fingrene fra!

Løsningen er variationer. "De0dkhmkth" betyder for eksempel "Der er ingen, der kan huske min kode til hjemmesiden", mens "Maeuahf0" betyder "Min arbejdskode er umulig at huske for nogen". God fornøjelse med spionsproget.



Vi skal bruge hemmelige adgangskoder flere steder, og de skal alle sammen være forskellige, hvis de skal være noget værd.

Hold dine private data for dig selv

Smil – du er på! Din rejse på nettet efterlader sig spor alle steder. Både på nettet og på din egen pc.

Dine adgangskoder er ikke de største hemmeligheder, din pc rummer. For dem kender du i det mindste selv. Men pc'en står også stille og roligt og opsamler oplysninger om dig, uden at du bliver spurgt. Oplysninger, som nysgerrige sjæle kan aflure pc'en på et øjeblik. I hvert fald hvis du ikke sletter dem forinden.

Hvor har du været i nat?

Internet Explorer indeholder en række hjælpefunktioner, som skal gøre det let og ikke mindst hurtigt for dig at finde dine yndlingswebsider. Desværre går det ud over sikkerheden ved samme lejlighed. En nysgerrig person kan nemlig finde ud af ikke så lidt om dine surfvaner på den måde.

Den simpleste og mest afslørende funktion er **Autofuldførelse**. *Internet Explorer* husker de webadresser, du har besøgt de sidste 20 dage, og foreslår automatisk at færdiggøre de adresser, du taster i adresselinjen. Det kan føre til uheldige afsløringer, hvis du for eksempel bruger arbejdspc'en til at kigge efter nyt job på nettet. Det kan blive nødvendigt, længe før du aner det!

1984-metoden

Den letteste måde at undgå ubehagelige overraskelser er at regne med, at du bliver set – og handle efter det! Hvis du går ud fra, at dine tastetryk og museklik kan læses på forsiden af avisen i morgen, har du i hvert fald ingen falske forventninger om anonymitet eller urørlighed. Lad være med at hente ulovlige film på KaZaA, hvis du ikke bryder dig om at få en efterregning fra rettighedshaverne, og fortæl så frivilligt kolleger og familie, hvilke sider du besøger på nettet, de har alligevel set det på din pc.

Når man indtaster de første bogstaver af en internetadresse, foreslår Internet Explorer selv lignende adresser, som er besøgt for nylig. Husk det, hvis du besøger jobsøgningssider fra arbejds-pc'en, chefen kan nemt sidde og kigge med!

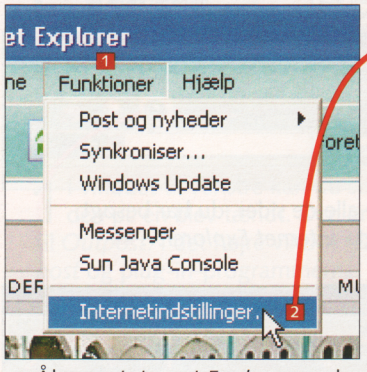
Faktisk husker *Internet Explorer* langt mere end blot en række adresser. Med et klik kan man fremkalde en komplet liste over besøgte websteder, sorteret alfabetisk og efter dato.

1 Hvis du ikke lige kan huske alle de sider, du har besøgt, så klik på knappen **Oversigt** i *Internet Explorer*... 1

2 ... så dukker en udførlig liste over websteder op, sorteret efter dato, og komplet med undersider 2.

Fjern sporene i Explorer

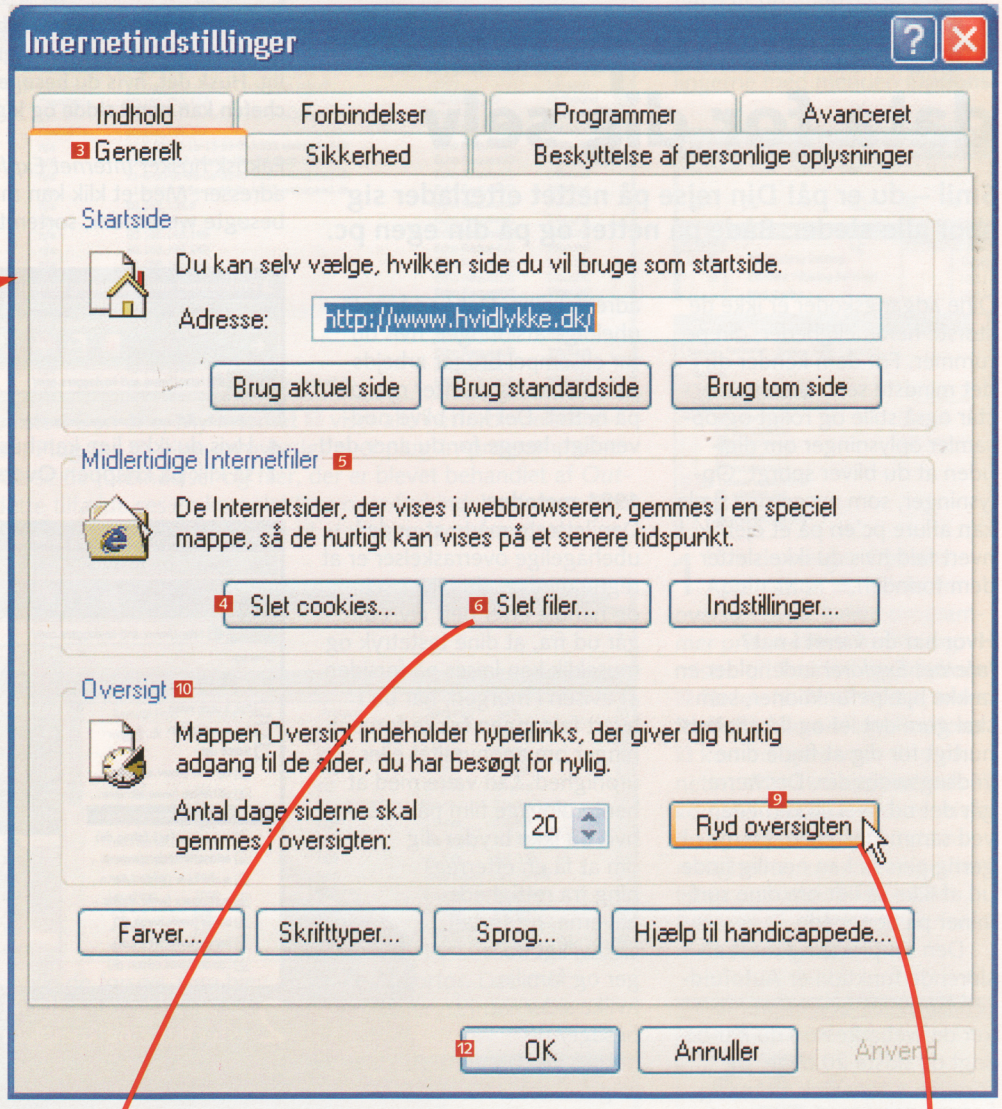
Heldigvis er det let at få *Internet Explorer* til at glemme, hvilke sider den har besøgt. Gør det til en vane at rydde op en gang imellem, hvis du er nervøs for at blive kigget over skulderen.

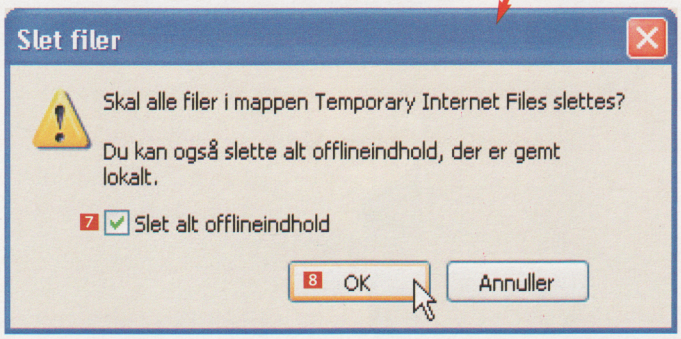


1 Åbn nu *Internet Explorer*, vælg menuen **Funktioner** 1, **Internetindstillinger** 2. Vælg endelig fanen **Generelt** 3.

2 Du kan vælge at slette cookiefilerne. Cookies er små samlinger af oplysninger, som du har indtastet på websider. Det er fristende at klikke på **Slet cookies** 4 og smide dem alle ud. En mindre dramatisk fremgangsmåde er dog at bruge *Ad-aware* til at fjerne de mest luskede af slagsen.

3 Find rammen **Midlertidige Internetfiler** 5. Klik på **Slet filer** 6 for at starte oprydningen.

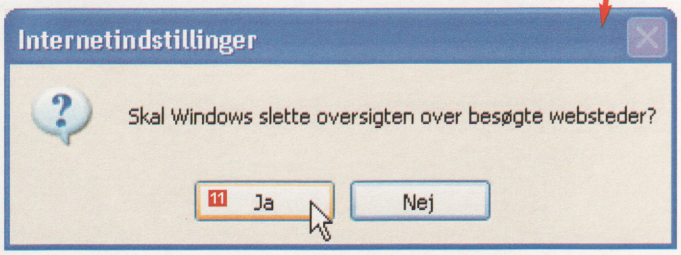




4 Sæt kryds i **Slet alt offlineindhold** 7, og klik på **OK** 8.

5 Sådan, nu begynder harddisken sikkert at arbejde intenst, mens filerne slettes. Efter et kortere eller længere tidsrum (der kan ofte gå op til nogle minutter) er alle de gemte (og glemte) internetfiler blevet slettet.

6 Tøm oversigten i Adresselinjen. Det gør du ved at klikke på **Ryd oversigten** 9 i rammen **Oversigt** 10.



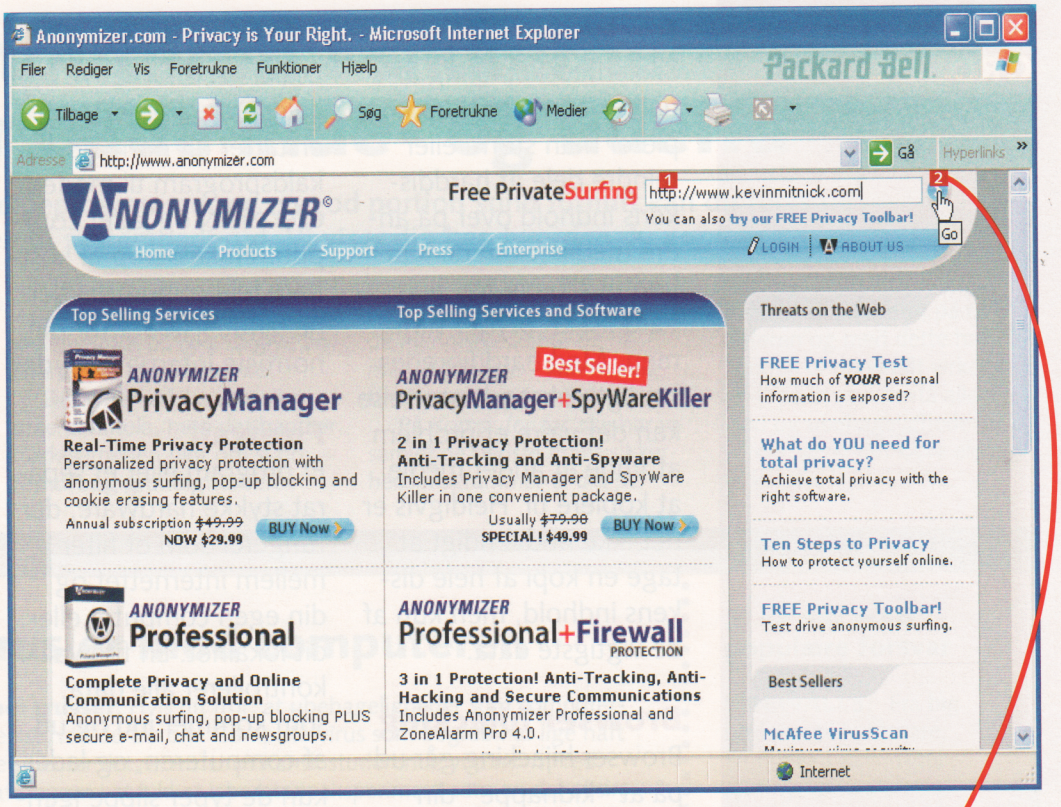
7 Nu spørger *Explorer*, om du ønsker at slette oversigten. Ja, det er lige det, vi er ude på! Klik på **Ja** 11.

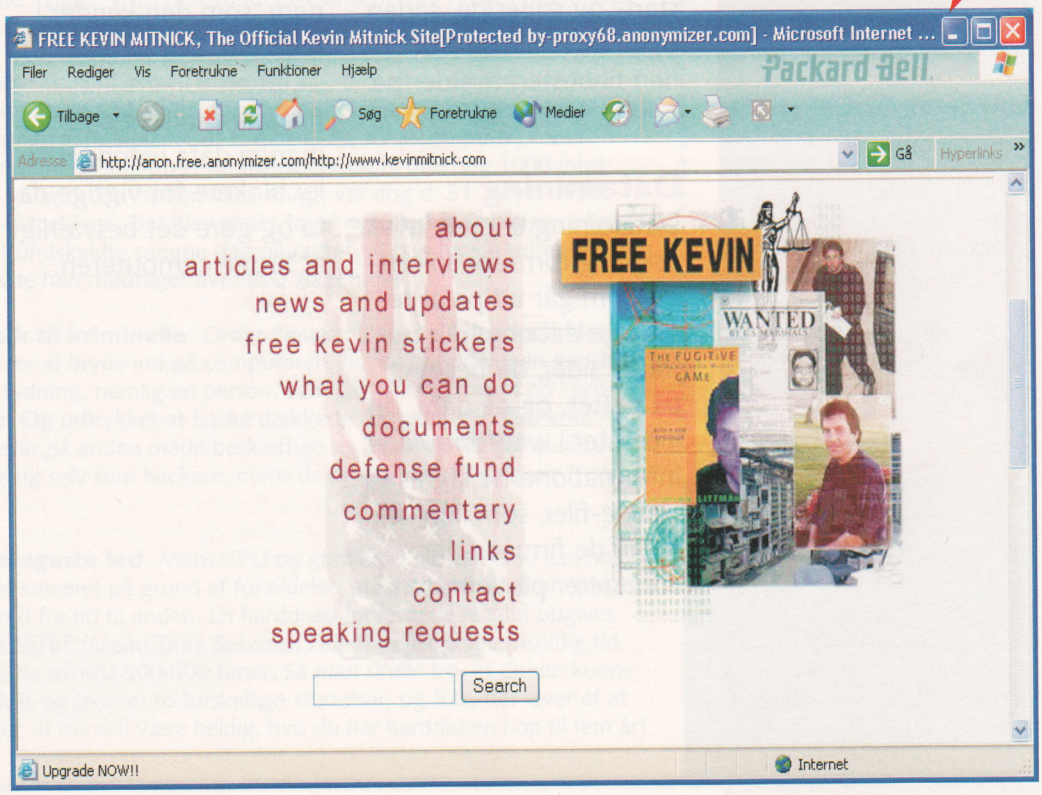
8 Slut af ved at klikke på **OK** 12. Dine spor er nu blevet slettet, og du kan roligt atter kaste dig ud i cyberspace.

Bliv anonym på nettet

Også ude på nettet efterlader du dig spor. Når du besøger en hjemmeside, bliver dit IP-nummer, altså pc'ens unikke netadresse, registreret. Sammen med din browsertype og -version, din e-mail-adresse og meget andet godt. Og selv om dit internetabonnement er af typen, hvor du får et tilfældigt IP-nummer, når du åbner for netforbindelsen, holder internetudbyderen styr på, hvem der havde hvilket nummer på et givent tidspunkt. Vær vis på det!

Vi kan ikke tilbyde dig fuldkommen anonymitet. Men i hvert fald gøre lidt for at hjælpe dig til at sløre sporene på nettet. Der findes nemlig firmaer, der har som mål at gøre dit surferi anonymt. Den mest navnkundige af de anonyme tjenester hedder Anonymizer, og de lader dig gerne prøve lidt anonymitet gratis. Hvis du får smag for det, sælger de software, der angiveligt kan gøre din pc komplet usynlig. I hvert fald så længe du er på internettet.





1 Åbn din browser, og vælg at gå ind på hjemmesiden: **www.anonymizer.com**

2 Nu får du *Anonymizers* forside på skærmen. Indtast den webside, som du vil besøge anonymt, i feltet **Free Private Surfing** 1, og klik på knappen **Go** 2.

3 Vi har her som eksempel valgt den officielle hjemmeside for verdens mest berømte hacker, Kevin Mitnick. Ham ønsker vi måske ikke ligefrem at udlevere vores IP-nummer til som den første.

Du kan nemt klikke dig videre fra en hjemmeside, som du ser gennem *Anonymizer*. Men du kan ikke se sider, som bruger programmeringssproget Java. God anonym netrejse!

5

SIKKERHEDS-ORDBOG

Begreber og grumme trusler, der er gode at kende til, når du vil sikre din pc.

Backup

Sikkerhedskopiering af data. Ved en backup kopierer man større eller mindre dele af harddiskens indhold over på andre medier, som de kan hentes tilbage fra, hvis harddisken bryder sammen. Med harddiskenes stadigt voksende størrelse kan det være et problem at finde et andet medie at kopiere til. Heldigvis er det ikke nødvendigt at tage en kopi af hele diskens indhold, men kun af de vigtigste data.

Browser hijacking

Browser hijacking går ud på at "kidnappe" din start- og søgeside, sådan at du automatisk ledes hen til bestemte sider på nettet.

Datamining

Datamining er en relativt uskyldig form for spionage, som går ud på at registrere data om dig ud fra de sider, du besøger på nettet, og de data, du indtaster i webformularer. Informationerne lagres i cookie-filer, som kan læses af de firmaer, der abonnerer på tjenesten.

Dialers

Dialers er alternative opkaldsprogrammer, som erstatter dit normale opkaldsprogram til modem eller ISDN og lader computeren kalde op til kostbare telefonnumre i fjerne lande i stedet for din normale internetudbyder.

Firewall

Et program eller et separat stykke hardware, der fungerer som et filter mellem internettet og din egen computer eller dit lokalnet. En firewall kontrollerer alle data, som kommer ind og ud af computeren, og lader kun de typer slippe igennem, som den kender i forvejen. Det betyder også, at en forkert indstillet firewall kan slippe for mange data igennem eller blokere for vigtige data og gøre det besværligt at bruge computeren.

Hacker

En hacker er en person, der trænger ulovligt ind i andre computere. Motivet kan være at forvolde skade, at stjæle oplysninger eller simpelt hen at se, om det kan lade sig gøre. I alle tilfælde er det ulovligt – og du ønsker næppe, at folk uopfordret sparker din hoveddør ind "for at afprøve sikkerheden".

Harddiskcrash

En harddisk er et fantastisk stykke finmekanik, men også ganske skrøbelig. Harddiskens læsehoveder befinder sig få tusindedele millimeter over diskoverfladen, og hvis de rører overfladen, er det slut. Så er både disk og data ødelagt. Og det er blot én af de mekaniske fejl, der kan ramme en harddisk. En dag sker det også for din nye harddisk. Så vær beredt, og tag en backup!

Keylogging
Med keylogging er vi i den farligere ende af spektret. Keylogger-programmer registrerer alle dine indtastninger og sender dem hjem til firmaet eller personen bag. På den måde kan adgangskoder og kreditkortnumre aflures.

Makrovirus
Microsofts Office-programmer kan udvides med nye funktioner ved hjælp af programmeringssproget VBA (Visual Basic for Applications). Men man kan også skrive virusprogrammer i VBA. Makrovirus optræder i Word-, Excel- og andre Office-dokumenter. Makrovirus er sjældent de farligste typer, men de er til gengæld lette at programmere og forbedre med nye ubehageligheder fra virusprogrammørerne.

Malware
Malware er en forkortelse for "malicious software" (ondsindede programmer).

Orme
Orme er en afart af virus, men kan i modsætning til almindelige virus selv udsprede smitten ved hjælp af internettet. Det sker oftest ved, at ormevirussen udvælger tilfældige navne i mailprogrammets adressebog og sender tilsyneladende uskyldige mails med vedhæftede filer. Man skal almindeligvis åbne den vedhæftede fil for at blive smittet, men enkelte ormevirus udnytter smuthuller i mailprogrammerne *Outlook* og *Outlook Express* og smitter ved modtagelsen.

Parasitter
Parasitprogrammer er alle slags snylteprogrammer. Udtrykket bruges som fællesbetegnelse for al den spyware, adware og andre programmer, der indeholder mere, end de ser ud til.

Spyware
Spyware er en fællesbetegnelse for programmer, der registrerer dine handlinger og giver besked til moderfirmaet.

Tracking
Tracking betyder "sporing" på engelsk, og det er netop, hvad det handler om: at følge dine spor. Det kan for eksempel ske ved hjælp af et lille billede, som er indeholdt i en reklame-e-mail (og som måske endda er usynlig). Billedet fungerer som en "spionsender", ved at websites, du herefter besøger, kan tjekke, om du har sporingsgrafikken liggende – og dermed følge med i dine surfvaner.

Trojanske heste
Trojanske heste spredes på samme måde som almindelig virus, men har ikke til formål at ødelægge pc'en, blot at overtage kontrollen med den. Det er særlige værktøjer, der smugles ind i pc'en maskeret som uskyldige programmer. Når de er installeret, kan de give hackere mulighed for at styre og overvåge din computer. Pc'en vil tilsyneladende virke som altid, men den trojanske hest kan ubemærket opsnappe vigtige data (fx kreditkortnumre) og sende dem hjem til ophavsmanden, når du går på nettet. Eller programmet kan "kidnappe" pc'en, så den kan bruges til hacking og angreb på webservere.

Virus
Computervirus er programmer, der har til formål at skade eller i hvert fald smitte din pc. Virusprogrammet smitter ved hjælp af andre programmer, som de hæfter sig på. Når du kører det angrebne program, kopierer virussen sig til din harddisk og går i gang med at inficere andre programmer. Nogle virus kan slette filer eller ligefrem ødelægge computeren, mens andre bare gør pc'en langsommere eller kommer med drillemeddelelser på skærmen.

SUCCESEN FORTSÆTTER

NU KOMMER ILLUSTRERET VIDENSKABS STORE ÅRBOG 2003

Illustreret Videnskabs store årbog stiller skarpt på alt det, som i 2003 forandrede vores verden.

Og du får hele året med - også de sidste måneder

SPAR 100,-

Som abonnent på KOMPUTER FOR ALLE får du din første bog for

KUN 59,50 +kr. 39,50 porto og eksp.

Normalpris 159,50 kr. + 39,50 kr. porto og eksp.

■ Årets profiler

Mød årets vindere og tabere, helte og skurke – bl.a. bjergbestigeren Aron Ralston, der skar sin ene arm af for at komme hjem.

■ Årets gang

Få overblik over hele året, måned for måned, uge for uge, dag for dag.

■ Året i tal

Se fx, hvor mange der søgte asyl i Europa, og hvad verdens dyreste telefonnummer koster.

■ Året i billeder

Oplev de største øjeblikke og de mest fantastiske pletskud fra hele verden.

■ Status 2003

Vi tager året til eksamen. Var det fx et godt eller skidt år for verdensfreden?

FANTASTISKE BILLEDER • UNIKKE ILLUSTRATIONER • MASSER AF BAGGRUNDSVIDEN • ÅRETS STØRSTE BEGIVENHEDER

ILLUSTRERET VIDENSKABS ÅRBOG/Bonnier Publications A/S. Kundeservice, 0900 København C, tlf. 39 10 30 56, www.kundeservice.nu Et Bonnier AB-selskab

SVARKUPON

☐ (1381) **Jeg er abonnent** på KOMPUTER FOR ALLE og bestiller Illustreret Videnskabs Årbog i løbende abonnement (leveres i slutningen af januar 2004). Jeg modtager velkomsttilbuddet til abonnenter og får 2003-udgaven for kun 59,50 kr. + porto og eksp.gebyr 39,50 kr., derefter modtager jeg hvert år i slutningen af januar en ny stor årbog for 159,50 kr. + porto og eksp.gebyr 39,50 kr. (med forbehold for prisændringer).

☐ (1382) **Jeg er ikke abonnent** på KOMPUTER FOR ALLE , men ønsker at bestille et løbende abonnement på Illustreret Videnskabs Årbog (leveres i slutningen af januar 2004) til ordinær pris, 159,50 kr. + porto og eksp.gebyr 39,50 kr. (med forbehold for prisændringer). Derefter modtager jeg hvert år i slutningen af januar en ny stor årbog for 159,50 kr. + porto og eksp.gebyr 39,50 kr. (med forbehold for prisændringer).

Navn: _____

Adresse: _____

Postnr.: _____ By: _____

Skriv venligst tydeligt – helst med blokbogstaver 0311

9353

Al kundeinformation såsom navne- og adresseoplysninger behandles vha. moderne informationssystemer og lagres hos Bonnier AB. Tilbuddet gælder ikke i Grønland, i udlandet og på Færøerne.

POST
Sendes ufrankeret
ILLUSTRERET VIDENSKAB
betaler portoen

ILLUSTRERET VIDENSKAB

Kundeservice
+++ 6094 +++
0900 København C